UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA,

v. 17 Cr. 548 (JMF)

JOSHUA ADAM SCHULTE,

Defendant.

Trial

----------x

New York, N.Y.
July 7, 2022
9:05 a.m.

Before:

HON. JESSE M. FURMAN,

District Judge
-and a Jury-

APPEARANCES

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
BY: DAVID W. DENTON JR.
MICHAEL D. LOCKARD
Assistant United States Attorneys

JOSHUA A. SCHULTE, Defendant *Pro Se*

SABRINA P. SHROFF
DEBORAH A. COLSON
Standby Attorneys for Defendant

Also Present: Charlotte Cooper, Paralegal Specialist

(Trial resumed; jury not present)

THE COURT: Good morning. I hope everyone is well. We should be ready to proceed to closings.

A couple quick things.

First of all, I will tell the jury, but I completely lost track of days yesterday when I said that we would go until 5:00 tomorrow. I'm actually going to end tomorrow at three, so you know, and I will let them know as well.

A couple things that we do need to address at some point today, although I don't think we need to do it right now, is the exhibits, whether everyone's in agreement on what came into evidence and whether we have collected all that.

Second, how we're handling the classified exhibit, not GX1 but the other one, and whether it should be marked as classified or not.

Third, and we don't need to discuss this, it is my intention to send the indictment to the jury, as I think you saw in the draft jury charge. So that should also be included with the exhibits and available electronically to the jury.

And then lastly, I think we've told standby counsel that Mr. Schulte's submissions from yesterday -- there were, I think, two -- need to get docketed. I want to make sure that they are filed on ECF in the near term.

All right. Ms. Shroff, good?

MS. SHROFF: Yes, we will. I explained why we

couldn't do it yesterday.

THE COURT: I'm not chastising; I'm just saying make sure they get filed expeditiously.

MS. SHROFF: We shall. We shall do it by end of day, maybe tomorrow morning.

THE COURT: Great.

Is the government ready to proceed?

MR. LOCKARD: Yes, your Honor.

THE COURT: And I take it, Mr. Lockard, you're doing the principal closing. Is that correct?

MR. LOCKARD: That's correct, your Honor.

THE COURT: All right. Do you still estimate two hours, maybe less?

MR. LOCKARD: I would say two hours.

THE COURT: OK.

All right. Anything to raise before we proceed?

Government.

MR. LOCKARD: No, your Honor.

THE COURT: Mr. Schulte.

MR. SCHULTE: I think I just need one minute in the back to change shirts.

THE COURT: All right. Why don't you go do that quickly now, and I'll get a report on the jury. And then we'll get ready to go.

Also, make sure you pull your mask up over your nose,

please.

All right. Mr. Schulte is back. We'll get the jury and get started.

(Jury present)

THE COURT: You may be seated.

All right. Welcome back. Good morning, ladies and gentlemen. I hope you had a pleasant rest of your day yesterday, and thank you for being here on time today.

Let me say a few different things.

First, one housekeeping matter.

Just so the record is clear, given that with my approval, only a first name was used, I just want to make clear that you've heard testimony during trial about Dave C. and you heard from a witness yesterday who testified under the name Dave. That is the same person. So Dave is Dave C., just to make that clear if it wasn't already clear to you.

Second, I just want to give you a heads-up that just as I've approved certain redactions or substitutions with respect to some of the exhibits you've seen, I've done that in very limited circumstances to the trial transcript as well, for reasons that you don't need to concern yourselves with or worry about. I'm just telling you that because during the parties' closings today, it's certainly possible that they will show you or reference a portion of the trial transcript that contains a redaction or a substitution. I just wanted to give you a

heads-up about that. As with the other redactions, you shouldn't speculate as to why. You did hear the testimony and you can consider it, and in that sense, your recollections govern. But otherwise, you should just treat it as redacted or a substitution.

One other housekeeping matter.

When I told you yesterday that you should be prepared to be here until 5:00 tomorrow, I completely blanked on what day of the week it was. Since we were starting on Wednesday, I got a little confused. I actually can't -- we can't -- sit until 5:00 tomorrow. So we will actually break tomorrow at 3:00 just for your planning purposes. We'll discuss your schedule more later, and that brings me to the last topic, which is the schedule, just so you have a sense of what today and tomorrow are going to look like.

As you know, we're at the stage where the parties will be giving their closing arguments. The way that works is the government goes first, then Mr. Schulte will go, and then the government has an opportunity to rebut Mr. Schulte's closing. That's because the government bears the burden of proof, so it gets the final word. And as you know, and as I will tell you again several more times, the government bears the burden at all times in this trial, and that's why it gets a rebuttal.

That's the way today will proceed. I'm guessing, and we'll have to play it a little bit by ear, but I'm guessing

we'll hear the government's closing, and then to ensure that you can give Mr. Schulte the same close attention that I'm sure you'll give the government, we'll take a 30-minute break, give or take, before Mr. Schulte's closing. And then depending on where we are, how long his closing is and so forth, we'll probably take a break, maybe a little bit shorter than that, but another break after his closing before the government's rebuttal. And then we'll see what time it is and whether I would have time to give you my instructions before the close of today or not.

We'll have to play it a little bit by ear, but that's the plan. And then once I give you my instructions, your deliberations will begin. And with the exception of tomorrow, when we'll end at three, I'll ask you to remain until you've either reached a verdict or until 5 p.m. each day after tomorrow. So just so you have a sense of what's coming down the pike, but we'll discuss that more as we proceed.

Why don't you ask my deputy at a break if you have a question, juror No. 13, and we'll take it from there.

With that, we'll proceed with closings, beginning with the government.

Let me mention to you, remind you, that what the lawyers say, what Mr. Schulte says, is not evidence. All right? You've now heard all the evidence. It's the testimony of the witnesses, it's the exhibits that have been admitted

into evidence, including the stipulations of the parties, but what the lawyers have said in their questions and what Mr. Schulte has said in his questions and their openings and now their closings is not evidence. All right? That's very important. Particularly Mr. Schulte, obviously, was involved in some of the events that you have heard about and that I'm sure both sides will discuss in their closings, but when he is talking about it in his closing, he's not giving testimony, he's not giving evidence; he's just making an argument based on the evidence that you have now seen and heard. So it's important to keep that in mind.

If their descriptions of any of the evidence differ from your recollections, it's your recollection of the evidence that governs. So, too, it's possible that they will make reference to what my likely instructions to you will be, and I will tell you, and remind you later, that if their description of my instructions differs from my instructions, it's my instructions that govern.

Having said all that, it's still important to listen to them with care. It's their opportunity to make arguments to you about what conclusions you should draw from the evidence to sort of tie it all together, since, obviously, it's come in in bits and pieces. So it's a very important and very helpful part of the process. So I would ask that you give them your undivided and careful attention.

With that, we will begin with the government.

Mr. Lockard.

MR. LOCKARD: On April 20, 2016, Joshua Adam Schulte stole the entirety of the CIA's highly sensitive cyber intelligence capabilities. The defendant -- at the time one of the CIA's own -- turned on his agency and on his country. Now, just days before April 20, the CIA had locked the defendant out of the secure restricted vault-like location on the network, where the files containing this data were stored. They had done that precisely because of the defendant's blatant violation of security rules and his abuse of his administrator authorities for personal ends.

But unknown to the CIA, the defendant had kept a secret cryptographic passkey. That passkey allowed him to bypass those restrictions, and he used it to execute a series of maneuvers on the network that gave him access, that allowed him to tunnel through to that network location, where files containing backups of the entirety of the CIA's cyber tool development were stored. He stole copies of those backup files. He searched for and deleted scores of log files in an attempt to cover his tracks, and then he reversed those maneuvers that had given him access to that location in an attempt to make it look like he was never there.

Now, shortly after stealing this extraordinarily sensitive intelligence information, the defendant transmitted

those backups to WikiLeaks, knowing full well that WikiLeaks would put it up on the internet. In the weeks following this break-in, the defendant took every step he would need to take in order to transmit those files to WikiLeaks. He downloaded a program that WikiLeaks itself recommends to leakers to use to send stolen data. He bought computer equipment to connect large hard drives to his home computer, large hard drives big enough to hold the backup files. He researched how to verify that large files had transferred over a network and how to confirm that they had transferred without errors or corruption. He downloaded and tested secure data deletion programs designed to nuke computers and destroy any trace of forensic evidence.

And after a couple of weeks, the defendant did just that. He completely wiped his home computers and any number of external hard drives. He preserved only the data that he wanted to preserve and made sure to leave no trace of anything else behind.

And on March 7, 2017, WikiLeaks began releasing that stolen data in a series of publications that it dubbed Vault 7 and Vault 8. Those releases were instantly devastating to this nation's foreign intelligence capabilities. Overnight, foreign intelligence cyber tools had to be shelved and rewritten. Ongoing operations had to be shuttered. Individuals -- human beings, who had assisted in getting these cyber tools onto adversary networks -- were put at risk of being exposed, of

being burned, of having their very lives in danger. The entire computer network the CIA used to develop these tools was switched off, unplugged, and seized by the FBI. This nation's foreign intelligence cyber capabilities had to be largely rebuilt from the ground up. And that national security catastrophe was the work of one man -- Joshua Adam Schulte.

Now, ladies and gentlemen, over the past several weeks, you have heard and you have seen devastating evidence uncovering the defendant's crimes, because despite his best efforts, despite his attempts to delete every trace of his deeds, he failed. The defendant left behind a trove of digital evidence, recovered by FBI computer scientists, that shows you step by step how he committed that crime. It's the computer equivalent of security camera footage. And in those cases, where there are gaps in the footage, you see step by step how it is the defendant who deleted that video.

Now, you've also seen how when WikiLeaks began publishing that CIA information that the defendant had stolen and transmitted, the defendant was quickly identified as a lead suspect. And it's no surprise why. While at the CIA, he had violated security protocols, he filed false complaints, he bragged about his ability to get himself access to the classified computer network, and he repeatedly went around or defied his supervisors and their instructions.

In November of 2016, several months after he sent the

stolen backups to WikiLeaks, the defendant left the CIA, angry and disgruntled. So after the Vault 7 release, the FBI sprang into action, quickly learning everything it could about the defendant and making arrangements to interview him. And during that interview, first held on March 15 of 2017, and in interviews that followed, the defendant lied. He falsely denied being involved in the leak of the CIA information. He offered up alternative theories about how the crime could have been committed that he knew were false. He attempted to divert the investigation's resources and attentions away from himself and down false paths.

Now, eventually, the defendant was arrested, and he was held at the Metropolitan Correctional Center, the MCC, here in Manhattan. And while he was here, as you heard during this trial, he had cell phones smuggled into the prison. He used those contraband cell phones to set up encrypted email accounts, to set up social media accounts under false names. He used services designed to disguise the location where the phone was being used and to allow anonymous access to the internet.

Using those tools, he sent a reporter documents that included sensitive information about the CIA's cyber groups, about its personnel. He drafted a series of tweets that included even more sensitive information about the CIA's cyber tools and started making arrangements to send those tweets out.

And this part of the plot, fortunately, was disrupted before it bore fruit, because the FBI learned of it and they seized the phones.

Now, ladies and gentlemen, you've also seen evidence of why the defendant did these things. And motive is not an element of any of the offenses; it's not something that you have to find during your deliberations. But nonetheless, the evidence does suggest to you why the defendant did this. It was ego and it was anger.

The defendant would like to think of himself as a bad ass, but in fact, he is a ticking time bomb, a nuclear bomb, one that was ready to explode at any perceived provocation or disrespect. And in April and May of 2016, the defendant, the so-called nuclear option, set out to lay waste to the CIA's cyber program, to prove his superiority, and to punish the people who he believed had wronged him. And in carrying out that revenge, he caused enormous damage to this country's national security.

Now, ladies and gentlemen, this summation is my opportunity to pull together the evidence that you've seen throughout this trial, to help explain how it fits together and how it leads inescapably to one conclusion -- that the defendant stole national defense information from the CIA; that he transmitted that information to WikiLeaks; that he lied to the FBI to obstruct the investigation; and that while in prison

he released and attempted to release more national defense information.

Now, before we talk about what the evidence shows, let's just have a brief overview of what the charges are. Now, you'll get detailed instructions about the charges from Judge Furman, and later in my remarks, we'll come back and talk about it in a little more detail there. But for now, let's just have an overview so that as we talk about the evidence you'll see how it's relevant and how it relates to the different charges.

The first set of charges relates to the defendant's theft and transmission of those backups from the CIA.

Count One charges illegally gathering national defense information, based on the defendant's stealing the CIA backups on April 20 of 2016.

Count Two charges illegally transmitting unlawfully possessed national defense information, based on sending those stolen backups to WikiLeaks.

Counts Five and Six charge computer crimes, based on how the defendant committed those crimes -- unauthorized access to a computer to obtain classified information, and unauthorized access to a computer to obtain information from a department or agency of the United States. And that's based on breaking into that network location, the Altabackups folder, on April 20, 2016, to steal the classified backups.

Counts Seven and Eight also charge computer crimes.

They charge causing the transmission of a harmful computer code or command, and that's based on the evidence that you've seen of the defendant executing commands on April 20 to delete data and to cause harmful changes to the network:

First, that series of reversions involving snapshots that had the effect of deleting about an hour and a half of the defendant's activities on the network; and second, editing and deleting numerous log files on the servers in an attempt to hide the actions that he had undertaken.

After the CIA theft and transmission charges, there's an obstruction charge, and that is based on the defendant's lies to the FBI in March of 2017 in an effort to obstruct or impede an ongoing grand jury investigation.

Finally, the prison transmission counts.

Count Three charges the defendant with illegally transmitting national defense information -- for sending notes and writings in an email to a Washington Post reporter, disclosing sensitive information about the CIA networks and personnel and the CIA's groups.

Count Four charges attempting to illegally transmit national defense information, based on writings that the defendant intended to publish, and took steps to publish, including tweets about sensitive cyber tools, about CIA tradecraft.

So before we get into the events of April 20, let's

just take one more quick break and talk about some concepts that are going to come up throughout the discussion, and it came up throughout the trial. And these are going to be important to help us orient ourselves as we go through the evidence.

First is the CIA's Center for Cyber Intelligence. You've heard a lot about this organization, and you've learned from this trial that this is the part of the CIA that does offensive cyber operation; that is, intelligence gathering, using cyber tools.

Now, you've also heard about some of the groups underneath the CCI. There's the Engineering and Development Group. That is the group that used the computer network that you're going to hear a lot about and have heard a lot about, the DevLAN network. That's the group that developed the cyber tools.

And you've heard the words "cyber tool" a lot, and by now you know that a cyber tool is a computer program. It's a computer program that's developed to gather intelligence on an adversary network.

Now, within the Engineering and Development Group, there's one group in particular you've heard a lot about, and that's the Operations Support Branch, or OSB. It is one of the five developer groups that operate underneath EDG, and it's important in this case because that is the branch where the

defendant worked for quite a period of time until he was transferred to another, sister branch, the RDB, and that's where some of the witnesses that you've heard from worked at the time -- Jeremy Weber and Frank Stedman. This is also the group that owned the server that hosted some of the services that the defendant unlawfully accessed.

And as you also heard from the trial testimony, OSB had a couple of particular areas of focus in their cyber tool development. One area of focus was quick-reaction tools; that is, tools that were needed on a short timeline for an imminent operation. You also heard that they had a focus on counterterrorism operations.

Now, I mentioned that network that the Engineering and Development Group used, the DevLAN. You've heard a lot about it. Let's just get the lay of the landscape on the DevLAN network.

DevLAN is a classified computer network used by EDG. Access to that network was limited. It was limited to the people who needed to access it for development, about 200 people in the entire CIA. And as you know, that system, as Anthony Leonis described, contains some of the CIA's most protected technical secrets, enabling the agency to conduct CNE, or computer network exploitation-related activities. That network was closed. It did not connect to the internet. It was accessible only from CCI offices, and it was accessible

only by cleared personnel with a need to know.

Now, why is that relevant?

That's relevant because one of the things you're going to have to decide is whether the information was national defense information. Now, you know it relates to the national defense because it relates to intelligence-gathering capabilities and this country's intelligence and military readiness. You also know that it's closely held because of all those protections, designed to keep that data secure.

Now, looking a little bit more underneath the hood of DevLAN, you know that the network was managed by ISB, and that will become important later, because there's going to be a transfer of power from the defendant to ISB.

You know that that network had certain computer programs that were used by developers called the Atlassian programs. Those are the programs like Confluence, which was a wiki for sharing information and documents and programs like Stash, which is where actual computer code and computer development documentation was stored.

And you know that the Confluence, which operated as a virtual server, ran on a computer server that was owned by the OSB branch. Now, you know that those programs, those Atlassian programs, were backed up. And during the relevant time period, they were backed up to a different location on the network that was called Altabackups. And you have heard and we will talk

about the defendant's efforts to get access to that Altabackups folder.

You've also heard a lot about administrators, and I want to talk about this for just a minute, because there are several different kinds, and it's helpful to keep in mind what kind of administrator we're talking about at any given point.

There are systems administrators that are responsible for the entire network -- the servers, the connectors, the desktops, that sort of thing. That's what ISB does.

Then there are the Atlassian administrators. Those are the people who configure those Atlassian products and have access to the servers where those products run, and their job is to help developers use the products, to set configurations for the programs and to control access to particular projects.

Now, you've heard through this trial that for a period of time the defendant was an Atlassian administrator, and we'll talk about what he did with that authority and what happened after he lost it.

The last type of administrator you heard about to a significant degree in this trial were project administrators, and that's something that applies to Stash. Right? Stash has projects that are different repositories for different projects. They're different tools, and a project administrator has authority over that particular project to set access for other users.

Now, you also heard a lot about the role of administrators and the importance of things like trust in an administrator. You heard about that from any number of people. You heard about it from Anthony Leonis. You heard about it from Jeremy Weber. You heard about it from Frank Stedman. You heard about it from the government experts.

Why is the role of an administrator important?

It's important because administrators, by necessity, have wide access to the network. They have access to things that an ordinary user doesn't have and doesn't need access to. And with that comes trust, especially on a network like DevLAN that hosted extremely sensitive cyber intelligence tools, cyber intelligence tools that were also subject to a need-to-know requirement because they were classified.

We're going to talk a lot about what it is that the defendant did with his administrator powers, and as we do that, I want you to remember what it is the other witnesses said about what type of administrator action is authorized and what type of administrator action is illegitimate.

The last thing I want to touch on briefly is classification. Classified information, as you heard at trial, is basically information that somebody in the government who is authorized to make that determination has found would cause serious harm to the U.S. national interest if it were disclosed. The reason that's important is access to classified

information requires a clearance and it requires a need to know it.

DevLAN was a classified system. It housed classified information. And as you'll hear in the charge given by Judge Furman, classification is relevant to whether documents are closely held, and it's going to be relevant to whether information was closely held after the WikiLeaks release of Vault 7 and Vault 8. And we'll talk about that when we get to the prison counts.

So let's talk about what the evidence has shown.

On April 20, 2016, the defendant used unauthorized computer access to copy CIA backup files and delete data.

The defendant then transmitted the stolen backup files to WikiLeaks, who began releasing it on March 7, 2017. He lied to the FBI and released, and attempted to release, more national defense information from prison.

Now, when we talk about what the defendant did on April 20, 2016, we're going to talk about digital forensic evidence. We're going to talk about different computer commands and different computer locations and different computer authorities that the defendant used.

And the how of what the defendant did can be complicated. There are a lot of different types of commands that we're going to talk about, and we're going to talk about why each one is significant. We'll talk about reversions.

We'll talk about data access and file copying. We'll talk about deletion commands. But what the defendant did is not complicated. All of those actions had a single purpose and a single plan, which was to get access to the backup files and copy them. And what it shows is this -- that after April 16, the defendant was not authorized to access the Confluence server, the OSB server, or the Altabackups folder as an administrator. Between April 14 and April 19, the defendant planned to get into the Altabackups folder and steal the backups. On April 20, the defendant did just that, and he copied the backup files. Also, on April 20, the defendant deleted data from OSB's server and from the Confluence virtual server.

Let's start with the defendant's loss of his administrator privileges.

It began on March 29 of 2016, when the defendant was transferred from OSB to RDB. And you heard a lot about why that was. Right? We don't have to get into it here. All that's relevant for your purposes about all those office conflicts, all those personnel disputes, all those complaints, what's important for you is the result, on March 29, 2016, was the defendant was transferred. He was transferred out of OSB and into RDB.

That's significant here because the Confluence server -- right -- the program that had one of those backups

that was stolen, ran on OSB's server. I mentioned virtual servers before, and you heard about it during trial. A virtual server is a computer within a computer. Right? It's virtual, meaning it's not a physical computer. It's a piece of software. The effect of that for your purposes is that having access to the physical computer that hosts the virtual computer does not give you access to the virtual computer. It's like walking into a room where there's another computer sitting on the desk. You can see it, you can pick it up, you can do things on the outside of it, but you have to separately log in to that virtual server. It's like a separate computer. And that OSB server was an OSB piece of computer equipment. It was managed by and it was administered by OSB. And after March 29, 2016, the defendant was not in OSB, and he was not an OSB server administrator.

You also heard about the defendant had his projects reassigned. Right? There were a couple of projects he was taking with him, but all of his OSB projects were staying with OSB. And you saw how his project administrator access, his ability to access those projects on Stash, were changed as a result.

Now, you also heard about some of the fallout from those changes and project permissions, and in particular, you heard about a confrontation that the defendant initiated over one of the OSB projects called OSB libraries. And on April 14,

the defendant approached Jeremy Weber and had a confrontation with him about it. The defendant found out he was no longer a project administrator for the libraries, and he was upset about that. In fact, he was so upset that after he went to talk to Jeremy Weber, he left to talk to the branch supervisor, Sean, came back and lied to Jeremy Weber about what Sean had told him. He lied and said that the branch supervisor said it was OK for him to be a project administrator. He was told no again. And as Sean confirmed, at no time did he ever tell the defendant he could have his administrator access back.

The defendant persists. Right? First, he sent an email, the third time he's told no by Jeremy Weber, copying Sean, the supervisor, and Anthony Leonis, his boss's boss, laying out what his privileges are on this project. And the defendant then asks if it would be OK to continue his accesses. And as you saw and heard from Anthony Leonis, the answer was, again, for the fourth time, no. It was a polite no. Anthony Leonis said this is going to be managed by somebody else, not by you. And so the defendant, minutes later, uses his Atlassian administrator permissions to change his own project administrator status, after he had been told four times no.

Now, OSB found out about this pretty quickly. Jeremy Weber saw that the defendant had done this and raised the alarm: "We have a situation with the libraries and the Atlassian products in general."

Now, I want to take a step back here, because what we've been talking about so far is OSB library privileges. And as you heard from the trial testimony, the only difference that being an OSB libraries administrator makes is that you can make permanent changes to the libraries directly. Not being an administrator just means you can still access the code, you can still use the code, but if you want to make changes, it has to go through a peer review process, a process to make sure that your changes aren't going to introduce bugs into programs of other developers who are using the libraries for their programs. It doesn't seem like that big of a deal.

Why is it a big deal?

Because at this point this is no longer about the OSB libraries. This is about the fact that the defendant, who has Atlassian administrator privileges, has just used those privileges to give himself access to something he was denied access to. It's like a bank manager finding out that an employee has been taking twenties out of the cash drawer. That's kind of a big deal, but if that employee has a key to the vault, then it's a very big deal. And on April 14, the CIA found out that Mr. Schulte had been taking twenties out of the cash drawer.

So they took immediate steps to take his key to the vault away. The deputy chief of the entire group, EDG, ordered that all developers in OSB be removed as administrators from

the Atlassian products. And it happened the next day, on Saturday. And you heard from the trial testimony about how two IT guys from ISB and Jeremy Weber came in. They changed all the passwords on all of the Atlassian servers, including Confluence, including Stash, how they changed the SSH keys -- right -- which is another way to log in. They changed those as well. Jeremy Weber was there to test all of his accesses and make sure that they'd been revoked, which they were. Not only that, but Mr. Weber changed the password to the OSB server, the server that was running the Confluence server.

So what does that mean?

That means that as of April 18, the defendant knows that he is not an administrator of any of the Atlassian products, and in fact, he's asked to verify that all of his keys have been destroyed. And he says that they have been. But as we'll talk about in a minute, he lied about that.

So after April 16, the defendant has no administrator privileges to any of the servers or to the Confluence server.

But what is he doing in the meantime?

In the meantime, he's already making plans to copy the backups. And he starts on April 15. Now, this is just one day after his confrontation over the OSB libraries. This is before he knows that his administrator privileges have been revoked.

What is he Google searching?

He's Google searching "Confluence admin view

restricted pages."

Now, why is that relevant?

That's relevant because, on Confluence, like in Stash, there are permissions for who can see different pages, and a normal user, their access is determined by what permissions are granted to them. But an administrator can see all the pages.

What restricted pages is Mr. Schulte interested in on April 15?

Well, all you have to do is look back to what he did on April 14. And what he did on April 14 was give himself unauthorized access to the OSB project. I think the evidence and your common sense tells you he's interested in OSB's Confluence page.

And why would he be interested in that?

Because there are passwords on that page. They're available to OSB developers.

What else does the defendant do on April 15 that shows his interest in OSB?

He logs in as an administrator to OSB's server.

(Continued on next page)

MR. LOCKARD: (continuing) Now, remember, he is not in OSB. He hasn't been in OSB for at least a couple of weeks. And, in fact, not only is he not in OSB, but nobody has logged into the OSB server as an administrator for almost six months before this date. This is not a regular thing. What reason does the defendant have to be logging into the OSB server as an administrator? There is no legitimate administrator purpose for this act. And what the defendant does next tells you what he is interested in. Actually, there are two things -- one thing that he does and one thing that he does not do.

Remember, at this time this is an OSB, not an RDB server. What does the defendant do next? He opens a second session as a regular user and he attempts to access the Altabackups folder from there.

Now, to realize the significance of this, let's talk about what the Alta backups folder was for. Right? It is to store backups. Kind of obvious. So why do you need access to the backups folder? There are just two reasons. One is to copy the backups so that they're stored there, the other is to restore backups. Backups are there as an insurance policy in case your computer fails, you lose your data, you can pull up one of the backups without losing that much time or work. The defendant is not doing either one of these things.

Ladies and gentlemen, I submit to you that this shows that on April 15th, the defendant was already thinking about

stealing the backups. Now, that attempt fails and you know why. As you heard from FBI computer scientist Patrick Leedom, there was one way to get to the Alta backups folder and that's from within the Confluence virtual server. The Confluence virtual server is the program that needs to write backup data to the backups folder and that's where the access point is. The defendant is trying to find out if he can get to Alta backups without being in the Confluence virtual server.

Now, that's what the defendant did and I want to remind you of what the defendant did not do. He did not close out his administrator session. When the defendant logged into the OSB server on April 15th as an administrator, he did not log out. He stayed logged in. And, in fact, it is that same session that he used on April 20th to steal the backups. So that's Friday, April 15th. As we already know, over the weekend the Atlassian administrator privileges were revoked from the developers and reassigned to the Infrastructure Support Branch. And the defendant gets that information on Monday. In fact, he gets a couple of pieces of unwelcome news.

First, he learns that he is not an Atlassian administrator anymore and he is told, along with the entire division, that ISB personnel are going to be the administrators of the Atlassian products and that there are two people who are going to do this and that their responsibilities include, among other things, the backups. Mr. Schulte is also asked to

confirm that he no longer has administrator privileges and he says that he does. How does he know whether he has administrative privileges? He tries them out. And in fact, he tries three administrator logins within minutes of each other: SSH key access to the Confluence server, SSH key access to the OSB server, and password access to the Confluence server. Two of those don't work, one of them does. On the 18th, he finds out that he still has that SSH key access to the OSB server but now he knows he can't log in to the Confluence virtual server anymore, the server he needs to be in in order to get to the Altabackups. But what does he tell the CIA? He tells the CIA that all private keys with access have been destroyed or revoked. He keeps that OSB key a secret. He lies about it. He also complains about it. He says: It seems like literally overnight all my permissions within the products were removed and all my permissions on the servers themselves were removed. Now remember, as he is saying this, he is logged into the OSB server as an administrator. And what is his complaint? It was done without informing him. Right? He is insulted.

He gets a second piece of unwelcome news on the 18th. He gets a memorandum from the CIA telling him that he has violated Agency security protocols and he has violated the position of trust that was given to him as an administrator, and he is given a warning: Do not attempt to restore or provide yourself administrative rights to any project and/or

system for which they have been removed.

If you will permit me to paraphrase just a little bit. He is being told you are not in OSB anymore, keep your hands off OSB stuff.

Now, Mr. Schulte gets this memorandum and he reads the description of his threat to Mr. Weber, remember, when he concluded that discussion on April 14th he told Mr. Weber I'm going to get my accesses back, you may as well just give them to me now. But, on the 18th, Mr. Schulte lies about it. He says, no, no I said I'm adding my accesses back until somebody with authority tells me otherwise. Now, ladies and gentlemen, you know that's a lie. You also know it doesn't make any sense because before he added his accesses back he was told, repeatedly, that he did not have permission to do so, including by Anthony Leonis.

So what does the defendant immediately start doing on April 18th? He starts researching copying large files over Linux and researching copying multiple files over Linux. Now, why is that significant? It is significant because the backup files are large and they are backups of Atlassian products which are Linux products. You have heard how Linux is just another operating system like MacOS or like Windows and it is an operating system that the defendant was very familiar with. In fact, that's the reason why he was asked to be an Atlassian administrator in the first place, because these are Linux

products.

What else does he do on the 18th? He uses that open administrator session to go into the OSB server and review files and delete files. What is he reviewing? He is casing the joint. He is doing surveillance to figure out what is there and he is deleting files to cover up the fact that on the 18th he was casing, he was casing the joint. And you can see here, between 6:32 and 6:49 p.m., he executes a number of commands called the VI command which you heard from Patrick Leedom which basically pops open a screen on the computer so you can see what is in the file. So he is opening up these log files to see what they're recording and he is deleting them when he doesn't like what they show. Right? He is figuring out where are the security cameras and how can I avoid them. Not only that, he goes specifically into the Confluence folder. Now remember, Confluence is a virtual machine which means it is a piece of software. Software runs in a folder or is saved in a folder and Mr. Schulte is looking specifically at what is in the Confluence folder.

Now, what is significant about that? What is significant about that is on April 16th, when the Atlassian privileges were being revoked from the developers including Mr. Schulte and were being given to ISB, they took a snapshot of Confluence before they did that. You have heard what the purpose of the snapshot is. It is a fallback. It preserves

the state of the system before you make changes so if something unexpected happens, you can revert back to that snapshot, no harm done. Mr. Schulte finds out that there is a snapshot. On April 18th he knows that there is a snapshot of Confluence taken from before he lost his administrator privileges.

Now, I want to touch briefly on the significance of some of the files that Mr. Schulte is looking at.

You have had an opportunity to see a lot of files documenting his activity on the OSB server and it is important to note where these came from. And as you can see and as Mr. Leedom testified, files like this come from shell.log fileslack. Now what is fileslack? Fileslack is where deleted data lives. You have heard about a couple of places where deleted data continues to exist and can be recovered even though it has been deleted by the user. Fileslack is one of those kinds of spaces. And what it means is that the shell.log file, which records the commands that the user is typing in on the keyboard, has been edited and these commands were deleted. Now why is that significant? It is significant because Mr. Schulte did not want you to see what he was doing. It tells you what he is up to. What he is up to is looking to steal data.

And if you look at Government Exhibit 1703-1, which contains some of the slides from Mr. Leedom's expert presentation, you will see throughout that presentation that

significant information, significant evidence is coming from fileslack, from unallocated space on Mr. Schulte's virtual machine, right, which is the VM he runs on his own desktop. And at the end of the day on the 18th, after he has done his reconnaissance, he closes the vault on the 8th floor of the RDB offices. What does that tell you? It tells you he was the last person in the office; he waited until the office had thinned out or everyone had gone home. The next day he does more Google research that is relevant to his plan to steal the backups. Now he is looking at hash algorithms.

Now, you heard from Mike Berger, an FBI computer scientist, what a hash algorithm is. It is math which we don't have to get into. What is important is its purpose. The purpose of a hash algorithm is to tell you whether two files are identical or even not identical. Even a small difference if the file data will give you a different hash algorithm result and so it is used especially when you are transferring files to see if it transferred directly, if it had corruptions, if it had errors, if it had dropped data. It is the kind of algorithm you would want if you are transferring large files like the backups and you want to make sure that they're not corrupted, which leads us to April 20th, the date of the break-in.

On April 20th, Mr. Schulte got some more unwelcome news. A division-wide e-mail goes out that the Confluence

server is going to be moved from OSB server to ISB network space. Now why is that important? It is important because Mr. Schulte still has that OSB administrative session open and that is the only thing that puts him in the same place as the Confluence server. Now remember, this server was only on OSB as kind of a historical accident. At the time that these programs were adopted and installed by the CIA, the OSB server was just a place that had enough space and enough firepower to run the Confluence program. It was never supposed to stay there, just like the Atlassian administrator privileges were never supposed to stay with the developers. But now that's changing and you know why. It is changing in response to Mr. Schulte. So he does not wait. He has already made his plans, he has already done his reconnaissance, he already has the blueprints that he needs. He has already scoped out where the security cameras are and he doesn't waste a minute. That night he steals the backups. And as you saw from Mr. Leedom's expert presentation, between 5:30 and about 6:00 p.m., Mr. Schulte executed a series of commands that restored his access to the Altabackups, copied the backup files from March 3rd, 2016, reversed those maneuvers, and deleted a bunch of log files.

Like I said earlier, it is a complicated series of steps but the purpose and the result is simple. So, let's look at the first part of that step.

Now remember, Mr. Schulte is logged in as an administrator to the ESXi server that is owned by OSB. That does not give him access to Altabackups. Right? He learned that a few days ago when he tried to access Altabackups from the OSB server and it failed. So what does he do? He reverts the Confluence server to April 16th. Now, between April 16th and April 20th there are no significant differences in the Confluence server except one. The one significant difference is that on April 20th, Mr. Schulte does not have access to the Confluence server and on April 16th he did. So he reverts the Confluence machine to the snapshot and you can see the command that he executed to do that. He takes a snapshot of the server as it exists before he makes any changes, he reverts it, he takes it back in time to April 16th, and then he logs in. Once he is logged in now he can get to the Altabackups folder.

Now, how do you know he logged in? One reason you know he logged in is shown here. He deletes log files from the Confluence folder. Why would he want to delete log files from the Confluence folder if he did not log in to the Confluence machine? This tells you that he is trying to hide his login. And you can see where the evidence of these deletion commands came from, they came from unallocated space on his computer meaning that he not only deleted the log files from the server, he also deleted files from his own computer. So once he is in the backups folder, you know what he did next. He copied the

March 3rd backups. One reason you know that is because those backups were in fact copied and they were copied on April 20th during the time that Mr. Schulte had that server in its reverted state. You also know that those were copied because they showed up on WikiLeaks.

Now, as you know, you are going to hear some argument from Mr. Schulte later today and I expect he is going to make a couple of arguments to you about the events of April 20th. And before I address the arguments I expect you to hear I just want to make an observation about arguments from Mr. Schulte in general.

As you have heard from Judge Furman and as you will hear again, Mr. Schulte has no burden to make any arguments to you at all. He has no burden to put on a defense case. He has no burden to do anything. The reason for that is that the burden always rests on the government up and until you deliver your verdict. And that is right, that is how the defendant gets a fair trial, and the government embraces that burden. But, if the defendant does choose to make arguments to you, you can and you should evaluate them critically the same way that you are critically evaluating what I am telling you now, and you can and should ask yourself: Do these arguments make sense? Are they based on the evidence? Or, Do they make no sense? Are they confusing? Are they illogical? Are they based on the evidence or did they invite you to ignore

evidence? Did they invite you to imagine things that could have happened that there is no evidence of?

Now, what I expect you will hear from Mr. Schulte is the argument that you have not seen at this trial --

MR. SCHULTE: Objection. That is what rebuttal is for.

THE COURT: Overruled.

MR. LOCKARD: I expect you will hear Mr. Schulte argue that during this trial you have not seen a forensic artifact documenting a login command to the Confluence server and you have not seen a forensic artifact of a copy command for the backup files. And I expect he will ask you to conclude from that that he didn't log in to the server and that he didn't copy those files. Now, he is right that those two forensic artifacts don't exist but he is wrong about the conclusion you should draw from that. And the reason he is wrong is because there is plenty of other evidence that he did exactly those two things. Right? We just talked about one of them. The files were copied and they were copied while Mr. Schulte had the ability to copy them so that's one reason you know that he copied those files and you know that he had to log in to the Confluence server to do that. Another reason is that he deleted and attempted to delete evidence of having done so. A third reason is that was his plan the whole time. As we have seen, from April 15th through April 20th, Mr. Schulte has taken

a number of steps designed to lead exactly to this point where he has access to the Altabackups folder and he can steal those backup files.

So the argument that you don't have those forensic artifacts -- to go back to our bank heist analogy -- it is a little bit like having security camera footage of the burglar getting into the bank, making himself a key to the vault, and then deleting the security footage from inside the vault. Right? The fact that there is no footage of what happened inside the vault is not evidence that he didn't go in there, it is the opposite. The fact that he deleted that footage is overwhelming evidence that he did go in the vault and that's what you have here. So let's talk about that deletion.

Between 5:55 p.m. and 6:58 p.m., Mr. Schulte systematically searches out and deletes numerous log files on the OSB server and you saw that during Mr. Leedom's expert testimony. You saw the RM command which is a Linux command that just means deletes. So every time you see RM, that's Mr. Schulte deleting a log file.

Now, you also heard testimony from a number of people about log files and their purposes. You have heard that from Mr. Weber, you have heard that from Mr. Leedom, you heard it from Mr. Stedman. And they all were uniform in the testimony that they gave you which is there is rarely, if ever, good reason to delete a log file. And on those rare occasions where

there might be a legitimate reason to delete a log file, the log files you would delete are the oldest log files. But, in Mr. Schulte's deletion of files he is both casting a wide net and seeking out the most recent files to delete. And Mr. Leedom described to you what some of these logs maintain and it is fair to say that it is a wide variety of log files that would record a wide variety of activity including the activity that the defendant is executing on that server that night. And again, just like he did on April 18th, he goes into the Confluence folder to delete Confluence log files.

Let's go back. Now, there are some log files he doesn't delete and you have heard testimony about how Mr. Schulte unsuccessfully searched for a log file called VIclient on the OSB server and he didn't find it. The reason he didn't find it is because he was looking in the wrong place. The VIclient log file is on his computer, not on the server. But what is important about the fact that he was looking for it? Well, you know that because the FBI found evidence in the VI log file that the defendant could not find. And what is shown in there is Mr. Schulte viewing snapshots of Confluence on April 20th. It shows Mr. Schulte creating a snapshot on April 20th. It shows Mr. Schulte reverting the Confluence virtual machine to the April 16th state. It shows Mr. Schulte re-reverting or undoing his reversion back to the snapshot that he took, that re-reversion that erases that entire period of

time when he was in the reverted state. It shows him looking for what snapshots are available and then deleting the snapshot that he took. This is the evidence that Mr. Schulte was trying to find on April 20th and this is the evidence that he did not want you or anyone else to see.

I mentioned earlier how Mr. Schulte is looking for the most recent log files to delete and there is an example of this here where you can see that he is specifically searching out files that were last modified during the time period when he has the Confluence server reverted and specifically deleting those files, the files that would have evidence of what he has been up to. And what is in those log files? Those VMware log files while he was in the reverted state? They contain evidence of exactly what Mr. Schulte was doing -- device connections, snapshot activity, data transfer logs. That is the kind of data that Mr. Schulte does not want you to see.

Now I am going to touch briefly on one issue. I think Mr. Schulte has suggested at times through his questioning that maybe somebody else was using his computer this entire time. I think you know very easily that that is not the case for any number of reasons. You know it, number one, because this is the administrator session that Mr. Schulte opened on April 15th. Right? This is the session that Mr. Schulte used on April 18th when he was conducting his surveillance. And, while Mr. Schulte is using this session on April 20th, he is also

doing other things on the computer. Right? He has one computer that is his DevLAN workstation, he has another CIA workstation right next to it, and while he is stealing the backups he is having IM chats with colleagues, he is sending e-mails to his boss. And when he is done, he is the person who badges out and locks the vault. There is no doubt that this is Mr. Schulte behind these commands and that Mr. Schulte stole these backups.

Now, as I mentioned a few minutes ago, motive is not an element but the question does come up in your minds: Why did he do this? We don't have to dwell on it because the evidence of what he did is, frankly, overwhelming. But I would submit to you that the evidence you have seen nonetheless suggests a "why," and the "why" is basically Mr. Schulte was having some problems at work, to say the least, in early 2016.

His main project, Brutal Kangaroo, was so habitually behind schedule that one of the tools earned the name Drifting Deadline. It was so behind schedule that the customer who had ordered that tool went and asked for somebody else to provide a replacement. And you heard testimony about that from Frank Stedman. That's the Almost Meat project. And how did Mr. Schulte respond to that frustration and disappointment? With confrontation and escalation, exactly the kind of traits that his colleagues had come to expect from him. He has a profanity-laced interaction with his supervisor, he barges his

way into a meeting, he lies about how long it is going to take for the competitor product to get the tools that it needs, and then afterwards, as you heard from Frank Stedman, he came up to Frank Stedman again and tried to get Frank on his side. Right? There was that component that Mr. Stedman was delivering that Mr. Schulte said oh, that will take six months and then Mr. Stedman spoke up in the meeting and said, no, it will take three weeks. After the meeting Mr. Schulte tried again; *Frank, don't you think it will take six months?* And Frank wasn't having any of it, he said no.

While that is going on Mr. Schulte's colleague, who is working with him on this project, Amol, who you have heard a little bit about, they don't get along to begin with. And as the frustrations with the Drifting Deadline project mount it turns toxic. Right? Mr. Schulte is filing complaints. He is escalating. He is filing threat complaints. He is escalating again. He is filing for a protective order. He is escalating again. In an interview with security he claims that he thought Amol was going to bring a weapon to work, that he was going to commit a mass shooting. And every time the defendant escalates it backfires, it results in him getting more isolated from his colleagues, it results in him getting moved from OSB to RDB which is not what he planned, so in early 2016 Mr. Schulte's frustrations are mounting. And then you saw what happened with the OSB Libraries project. And after escalating and escalating

and escalating in April of 2016, Mr. Schulte exploded. You have heard about it from his own words when he told Mr. Weber: I will eventually get my access back to the libraries and that access should just be enabled now.

You heard about it from Mr. Leonis. Schulte told him he felt his privileges were being removed unfairly and he wasn't going to allow it to happen and he would fight back.

You heard about it from Mr. Roche who is, at the time, literally about three people away from the director of the CIA, and Mr. Schulte told Mr. Roche: I could restore my privileges if I wanted to. You know I could do that.

And, you saw Mr. Schulte himself in that videotaped interview with security. Now this is April 8th of 2016. This is even before the OSB Libraries incident but it shows you the context and the mindset that Mr. Schulte is in. According to Mr. Schulte: Access doesn't really apply to me, essentially, is how it works. So I can get -- they can go through and they can remove my permissions but I still have full permission to everything. He says I feel like there definitely needs to be some kind of punishment for my management for treating me like this and some kind of apologies. When I feel like I'm being punished for something that I don't think I should be punished for and no one seems to have my back and everyone is always against me, I feel like I'm going to do whatever I have to do to make the situation right. So April 20th represents the

Nuclear Option going off.

Now let's turn to the evidence that tells you that Mr. Schulte then transmitted the stolen backups to WikiLeaks.

Now there is some, again, somewhat complicated digital forensic evidence that is involved in this phase of the offense but in reality this is pretty simple. If you find -- and I submit to you that the evidence compels you to find -- that Mr. Schulte stole the backups, that it is very easy for you to find that he transmitted the backups to WikiLeaks. That is because WikiLeaks got the backups and they released them and that, frankly, is all you need to know but that is not, in fact, all that we know.

So you know that the defendant copied the March 3rd, 2016 backups. Right? You know that those are the very same backups that WikiLeaks released data from. You know that in part from Mr. Leedom's testimony. Remember he testified about how the backups were broken, there was an error in the program that created the backups that resulted in missing data and some of the data that was in the backups that was supposed to be linked up was not linked. And the WikiLeaks information had exactly the same errors. So we know that what they released came from a backup and we know that it came from the backup the defendant stole. You heard the testimony of FBI computer scientist Michael Berger, who went through an extensive analysis, and determined that the data in the leaks came from a

window between the afternoon of March 2nd and the early morning of March 3rd. And you know that the March 3rd backups that the defendant copied fall right within that window.

But, the evidence has shown you more. It has shown the steps that the defendant took to transmit those stolen backups. On April 18th, the same night that he is casing the OSB server using that secret administrator login, he is also installing an updated version of TOR. TOR is that anonymous browser that WikiLeaks recommends to be used by leakers. On April 24th, after he has stolen the backups, he downloads Tails. That's another program that WikiLeaks recommends. It is a program that allows you to operate your computer without leaving any trace of what you have done while you are operating it. It is an amnesic system, it forgets everything.

Between April 23rd and April 38th, Schulte tested a secure file deletion program called Eraser Portable and he securely deleted a folder called Brutal Kangaroo on his home computer. And you heard that he queued up additional backup folder files to be deleted but closed the program without deleting them. But you also heard how even though he did not use Eraser Portable on those files, they were securely deleted because the FBI forensic review found no trace of those files when his computer was seized. You heard how he downloaded Darik's Boot and Nuke which is designed to nuke a hard drive. And he researched various Western Digital wiping utilities.

In addition to data deletion, he also researched how long it takes to calculate a hash value for large files. Again, that's how you tell that a file transferred correctly -- and the backups are large files.

And, on May 5, 2016, the defendant formatted his home computer after having wiped the drives. And you also heard how seven other external hard drives were recovered from his apartment, all of which has been wiped.

Now again, I expect that Mr. Schulte will make some arguments to you about the fact that there is no forensic artifact showing his transmission of a file to WikiLeaks and that there is no forensic artifact of his communicating with WikiLeaks, and that there is no forensic artifact of stolen CIA data on his home computer. But that is not evidence that he did not do those things. The fact that he deleted that evidence is proof that he did it.

How else do you know that he did it? Well, as we have already talked about, the backups were stolen in April of 2016 but weren't released by WikiLeaks until 10 months later. And you know why that is. It is because of that broken state of the backups and you heard from computer scientist Patrick Leedom that it is an effort to try and rebuild those broken backups and it took WikiLeaks a lot of effort to get it ready to publish.

But, in the meantime, the defendant is getting

anxious. He wants to know when is the stolen data going to start to come out. And you see from his Google search history before July of 2016 he had about two searches for WikiLeaks, I think they were both in 2010; and then one search in July of 2016 about the Clinton e-mails from the Democratic National Convention hack. Starting in August, he is extremely interested in WikiLeaks. There are 39 WikiLeaks-related searches in that four-month period or five-month period. There are 115 page sites. Ask yourself, why is he suddenly so interested in WikiLeaks? I think the evidence suggests the answer to you, he wants to know what has happened with the stolen data that he sent and when is it going to come out.

Now you also heard a lot of evidence about the effect that it had when the Vault 7 release did come out. You have heard about that from multiple witnesses. You heard about it from Anthony Leonis. You heard about it from Jeremy Weber. You heard about it from Rick Evanchec. I think Mr. Roche summarized it best when he said that the release was devastating. It was pulling off operations overnight, the vast majority of the operations that we were conducting. The vast majority because the sources and methods and, most importantly, the techniques that we were using to maintain clandestine signature, which is no one can see the signature, that cloak has been completely -- that information was now out in the public and we did know that there was great interest by

adversaries in this information. And so, the risk became too great to continue an operation that relied on this technology that was now out in the open and known.

It was devastating.

We have spent quite a while on the defendant's theft and transmission of the backups to WikiLeaks, let's turn our attention to some of the other charges that you are going to consider. First let's talk about the obstruction charge.

Now, you heard during this trial that the defendant was quickly considered a lead suspect because of the, let's say, tense relationship he had with the CIA when he left and because of his abuse of security protocols while he was there. So the FBI interviewed him. You heard that that first interview was on March 15th of 2017, about a week after the leak starts. That interview happened in a public place, it happened in a restaurant in midtown. You heard from Special Agent Evanchec that it was a voluntary and friendly interview, but you also heard that Mr. Schulte was extremely nervous.

Now, what happened during that interview? The defendant said a few things that are relevant to your deliberations. He denied being responsible for the leak. He said that his diplomatic passport was at home. Remember you heard testimony that Mr. Schulte had a diplomatic passport which is a special U.S. government employee passport as a result of his employment at the agency and that he did not turn

it in when he left? During his interview with the FBI he said it was at home. Now, that was false because they did not find it when they searched his apartment and they, in fact, later found it at his office in Bloomberg. So you know that when Mr. Schulte said his passport was at home it was either on him at the time or it was still at the office. But, you know he lied.

He said that he didn't have a copy of an e-mail that he had sent to the CIA's Office of Inspector General. You heard about that e-mail from Special Agent Evanchec as well. It is an angry e-mail that Mr. Schulte sent on his very last day in the office that he printed out and that he took home with him. And on March 15th, he said that he didn't have a copy of that e-mail and, as you heard, a copy of that e-mail was found in his home, and not just anywhere, it was found in the headboard of his bed, inches away from his head where he left.

And at the end of that interview at the restaurant, Mr. Schulte was given a grand jury subpoena. He was given two; one for his testimony and one for his cell phone.

Now, Mr. Schulte spoke with the FBI again, this time at the U.S. Attorney's office. He was interviewed on March 20th and 21st, back to back interviews. And during those two days Mr. Schulte was asked how the leak could have happened. And what's important to you is he offers up some ways that he

knew the leak did not happen because he committed it and he knew how it happened. So why is he giving false explanations for the leak? Because he wants to divert the investigation away from what he did. He wants to draw suspicion away from himself.

He was also asked about log files and Mr. Schulte said that the FBI should go look for certain types of log files that would show activity related to the theft of the CIA data. Now why is that important? Because Mr. Schulte believes that he has deleted all the log files. Right? He thinks this is another false trail.

And finally, the defendant denied, in every way possible, that he had anything to do with the leaks, whether he had stolen the data, whether he had been in communication with WikiLeaks, whether he had done anything that made the system at the CIA vulnerable to compromise. And he said no each and every time. And, as you know, each and every time he lied.

Now that is especially significant at the state the investigation was in in March of 2017 which is still barely weeks after the leak happened. This is at a time when the FBI doesn't know exactly what was stolen, they don't know exactly when it was stolen, and they don't know how it was stolen. And as you heard, this was a wide-ranging investigation considering any number of suspects, considering any number of possibilities, leaving no stone unturned. And the

investigators were considering every piece of information that witnesses provided including information provided by Mr. Schulte.

Now, despite Mr. Schulte's false statements, there did come a time when he was arrested and, as you heard, he was imprisoned at the MCC. And as the Judge has already instructed you and I will expect he will instruct you again, the fact that Mr. Schulte was in jail at the time is not relevant to the consideration of the evidence of his committing these offenses. It is evidence of where he was when he did it.

Now, you have seen some writings that Mr. Schulte made while he was in prison. These writings give you a window into his mind about what he intends to do. In one writing he says I will look to break up diplomatic relationships, close embassies, end U.S. occupation across the world. What can you take away from that? Well, how would Mr. Schulte be able to do those things, right? What kind of leverage does Mr. Schulte have? The leverage that Mr. Schulte has is whatever classified information he knows.

In a later writing he writes: Got to use last night. As you learned from the trial, he was talking about a cell phone that was smuggled into the prison. He says: The way is clear. I will set up a Wordpress of JoshSchulte.wordpress.com and presumptionofinnocence.Wordpress.com. From here, I will stage my information war.

Now, you also heard from Mr. Betances who was another inmate at the MCC who said he heard Mr. Schulte talk about an information war on a couple of occasions and both times, as soon as somebody else came around, Mr. Schulte clammed up. Now what does that tell you about what Mr. Schulte means by information war? It means that it is something that he doesn't want other people to know what he was doing.

There is more. Mr. Schulte goes on to describe in another article that he wrote what it is that he intends to do. And here he said the FBI, in all its brilliance, has just taken a senior engineer, with intimate knowledge of the NSA, CIA, and all project and operations he has worked on. What is he referring to? He is referring to classified information that he knows. And he goes on and says, does that sound like the most intelligent move? Really? Obviously this isn't intended as a threat. Well, let's pause here for a moment, ladies and gentlemen. You all have common sense and you all know that when somebody says something bad is about to happen but it is not a threat, it is usually a threat and that's exactly what this is.

Mr. Schulte goes on to make it even more clear. He says essentially it is the same as taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart.

Now, Mr. Schulte is not a soldier in the military, he is a former CIA officer and he doesn't have a rifle. He has classified information. That is his bullet.

And you also saw in one of the draft Tweets that Mr. Schulte had written: Until your government protects you and honors your service, send all your government secrets here: WikiLeaks.

So how does Mr. Schulte go about it? Well, first, as you heard, he smuggled in a contraband cell phone. And you heard about that from Mr. Betances. You saw a video of Mr. Schulte using that cell phone and you saw pictures of the cell phone. You saw the encrypted messaging apps that were on that phone like Signal and WhatsApp. You saw the virtual private network that was on that phone to disguise its IP address. You heard about how Mr. Schulte said that he could change the IMEI number. Right? That's the unique identifying number assigned to each phone, it is a way to disguise what phone you are using. And he talked to Mr. Betances a little bit about the CIA and he said that they had betrayed him and that he felt humiliated over what they had done to him.

So what does Mr. Schulte do with that phone? He sets up an encrypted ProtonMail account with anon12044 as the e-mail handle and he starts to use that account to communicate with a Washington Post reporter. And in those e-mail communications on September 24th of 2018, the defendant sent the reporter an

e-mail containing national defense information. This is the e-mail we are going to focus on for Count Three, the transmission of NDI from prison.

The NDI, the national defense information that Mr. Schulte sends, is information about two groups in CCI: EDG, the Engineering and Development Group that develops cyber tools; and COG, the group that deploys those cyber tools in operations. He identifies those two groups. He identifies the number of people in each group. And he talks about the architecture of the network that allows those two groups to communicate with each other.

Now, how does this relate to the national defense? Well, Mr. Roche talked about how it relates to the national defense. The number of employees that the CIA assigns to particular groups or particular missions is considered classified. Adversaries can take a mosaic of information with that piece and then start working backward to say for what this number is, where do we think these people are? What do we think activities we are seeing are associate with this kind of mission? What do we think this group does specifically? How can we target those individuals if we get some bit of information or understanding that someone has a connection with this group?

It helps adversaries start to unravel where the U.S. intelligence priorities are, how they're resourcing it, and

how, potentially, to start to identify the people who were involved in it. But, that's not all. Mr. Schulte anticipated and planned to release even more national defense information. He set up a Twitter account with the handle "Free Jason Bourne." Right? It is an account that he wrote down in his notebook and he wrote down the password to that account. And then he started talking about Bartender. So let's talk a little bit about Bartender.

As you heard from Jeremy Weber, Bartender is the name of a CIA cyber tool that was designed for human-enabled operation. That means people. In a human-enabled operation there is a person who is helping get that program onto the target network. And you also heard that Mr. Schulte played a role in Bartender. It started out as Mr. Weber's project but then Mr. Weber invited Mr. Schulte in to work on it too.

Mr. Weber also talked about the dangers of something called attribution. You heard a lot about attribution at trial so I am just going to summarize it briefly here. Attribution means identifying the CIA as being behind a particular operation or a particular tool. And you heard that attribution is a huge concern for developers. It is a big risk that they spend a lot of time to try and mitigate because the problem is if a tool or an operation is attributed or associated with the CIA, it creates a lot of risks. It creates a lot of risks of identifying other operations, of identifying other tools, and

in particular, of identifying the people who were involved in them.

And as you heard from Mr. Weber, Mr. Schulte was well aware of this risk as well as all of the developers and it was a regular topic of conversation in cyber tool development.

But what does Mr. Schulte do? Mr. Schulte starts drafting a series of versions of a Tweet where he intends to release information about Bartender that would attribute it to the CIA. Right? In one draft Tweet he says vendor, tool from vendor report, Bartender. He keeps reworking the Tweet. Just to authenticate me first. The CIA was involved in -- blank. The code for initially-planned cyber operation is in Vault 7. Additionally, tool described in vendor report is in fact Bartender, a CIA tool set for operators to configure for deployment.

Let's just touch for a minute on what Mr. Schulte says there. As you have seen in other portions of this notebook, this is a Tweet drafted in the third person. He is writing this in the voice of somebody else, somebody who claims to be his own colleague at the CIA because he is going to falsely claim that Joshua Schulte is innocent. What does he say in the tweet? He says: Just to authenticate me first. What is he trying to authenticate? He is trying to persuade people -- he is trying to persuade people that he is really a CIA officer. So how does he do that? He is going to do it by revealing

information that only a CIA officer would know. Right? Mr. Schulte knows that this information is not public. It does not authenticate you as a CIA officer to talk about something that you can find on Wikipedia.

Mr. Schulte continues to redraft the Tweet @vendor discovered tool in 2016, which is really the CIA's Bartender tool suite. Bartender was written to deploy against various targets. The source code is available in the Vault 7 release.

Now, you have also heard about why there is still a serious risk to this kind of attribution publicly identifying a CIA tool with a public report, right, about a piece of malware found in the wild. And it is exactly that attribution risk. And as Mr. Weber testified, right, to this day, he is not aware of the tool described in the vendor report ever having been publicly identified as Bartender. It has never been identified as a CIA tool and that is exactly what Mr. Schulte intends to out. He doesn't just intend to do it, he takes steps to do it.

As you know, he opened the Twitter account. He also opened a Buffer account that is linked to that Twitter account. Buffer is a service that allows you to pre-schedule Tweets to be released in advance on a schedule. He writes notes to himself about what he plans to do. He wants to finalize copy by Friday. He wants to edit during the weekend. Right? He wants to DL disk UL WL. Now, the interpretation of that phrase is for you guys to decide, but I would submit to you that that

is just shorthand for download discovery, upload to WikiLeaks. He wants to schedule Tweets on the 27th, send tech reports, Russia piece. Right? He is writing out his to-do list. He is taking affirmative steps to get these Tweets out and into the public. Now, he never does. Right? He is writing this schedule for September and at the very end of September and the beginning of October the phone is seized.

Mr. Schulte is also working on another publication, an article that he calls "Malware of the Mind," and in his notebooks he talked on several occasions about reworking various articles to get them out and into the public including the tenth article "Malware of the Mind."

(Continued on next page)

MR. LOCKARD: And this article, again, contains sensitive information about CIA cyber tradecraft. And again, you heard from witnesses about the attribution risk, not necessarily that the techniques themselves are sensitive, but that it is sensitive to disclose that the CIA uses them or to publicly allege by a former CIA officer that the CIA uses them. He talks about disguising data, where in the file system he would disguise data, how he would use crypto, all things that would be useful for an adversary to attribute to the agency.

Now let's turn back again to the charges and talk about what it is you have to decide in order to reach a verdict. Again, just a reminder about what each count charges.

Count One charges illegally gathering national defense information, based on having stolen the CIA backups on April 20, 2016.

Count Two charges illegally transmitting unlawfully possessed NDI, based on sending the stolen backups to WikiLeaks.

And then Counts Five and Six charge essentially hacking, unauthorized access to a computer to obtain classified information or information of a department or agency of the United States. We've talked about these at length.

Counts Seven and Eight charge causing harmful computer commands to a protected computer, based on the deletion of data and the elimination of data from the DevLAN system.

So for Count One, what you need to find is that the defendant stole the CIA backups on April 20, 2016; that he was not authorized to take them; and, having taken them, he was not authorized to keep them.

You should consider whether the backups contained NDI, which at this point, I think, is not likely to be seriously contested. It's national defense information. It's intelligence information. It is closely held on a highly guarded network. It relates directly to this nation's intelligence-gathering capabilities.

You'll be asked to find that the defendant had reason to know that the information in the backups would be used to injure the United States or to aid a foreign country. And you've heard a lot of testimony about the injury that the WikiLeaks release caused to the United States, which I submit to you is readily foreseeable to the defendant. And you've heard testimony about the assistance that this kind of information provides to adversaries, including foreign countries.

Finally, you'll be asked to find whether WikiLeaks was authorized to receive the backups. And there's really no doubt about that.

For the hacking counts, you'll also be asked to find whether the defendant's access to those backups was unauthorized, and you know that it was for any number of

reasons that we've talked about. You know that on April 20 he was not authorized to be in the backups folder. You know that on April 20 he was not authorized to be in the Confluence virtual server that he had to go into to get to the backups folder, and you know that he was not authorized to have an administrator session on the OSB server.

For Count Five, the question you'll be asked to decide is not whether the information was NDI, but rather, whether the information was classified. And you've heard ample testimony about how that information was classified.

Then, finally, for Count Six, you'll be asked to decide whether the backups were information from an agency of the United States. And again, there is no doubt that that information was information of the CIA.

For Counts Seven and Eight, the key question you'll be asked to decide is whether the computer commands that the defendant executed caused harm to those systems. Each count charges a different kind of deletion, in effect.

Count Seven charges a harmful computer command from, first, reverting the Confluence server back to April 16, spending an hour and a half in a reverted state, then re-reverting to April 20, eliminating all evidence of what happened in that hour and a half, and then deleting the April 20 snapshot. I think you've heard a lot of testimony about how that is harmful to the computer system. It impairs the

integrity and availability of data, and in fact, as you have seen, did, in fact, impair the availability of data, which was the point.

Count Eight charges harmful computer commands from deleting log files. You've seen evidence of so many -- so many -- log file deletions that occurred on April 20, 2016. And again, the point of each and every one of those was to eliminate data and prevent it from being available not only to system administrators but also to investigators and, ultimately, ladies and gentlemen, to you.

For the obstruction charge, this relates to lying to the FBI to obstruct or impede a grand jury investigation. So you'll be asked to find, did the defendant make false statements -- and we've talked about a number of false statements the defendant made -- and you'll be asked if he did so to obstruct or impede a grand jury investigation.

I want to talk to you just for a second about the grand jury investigation and the nexus of his false statements to that investigation. In particular, I want to focus your attention on the grand jury subpoena that he received at that interview at Pershing Square, that restaurant in midtown.

Before the defendant received that grand jury subpoena, he certainly knew there was an FBI investigation. He had googled it. He had read internet articles about it. When he met the FBI that day, they told him they were investigating

the Vault 7 release. When the defendant receives the grand jury subpoena, there could be no doubt at that point that he also knows this is a grand jury investigation. He received the grand jury subpoena for his phone and for his testimony, so he also knows the grand jury is certainly interested in what he has to say. And you can find from that that when he goes on to make false statements to the FBI, he has every reason to expect, and in fact, to believe, that those statements will go before the grand jury and that his false statements were intended to obstruct the grand jury's investigation.

Now, you heard he also lied before he received the grand jury subpoena, and you can consider that in determining what his intent was in his lies after he received the grand jury subpoena. Before he received the subpoena, he lied about his diplomatic passport. He lied about the OIG email. He lied about whether he had committed the theft. He did all of those things to impede the FBI, and he had the same state of mind after he received the subpoena. His intent was to obstruct the investigation and impair the investigation.

Finally, the two prison counts:

Count Three charges unlawfully transmitting unlawfully possessed national defense information. And here, you'll be asked to find if the defendant unlawfully possessed documents, writings, and notes pertaining to the national defense and whether he unlawfully transmitted them to a person not entitled

to receive them.

Now, here, the defendant is taking information that he knows in his head, and he is committing them to a writing. He's committing them to an email, and when he does that, he's not lawfully entitled to retain that email. That is unlawfully possessed documents, writings, and notes.

Now, you'll also be asked to find if the information in that email was national defense information. Now you know from the testimony of Mr. Roche that it was, or pertained to the national defense; that is, information that's useful to adversaries and that relates to our intelligence-gathering capabilities. You'll also be asked to find if it was closely held.

I expect the defendant is going to argue to you that it was not closely held because that information was already public. And that argument is wrong for a couple of reasons. I do not expect the defendant to be able to show you any evidence that the specific information in that email was publicly available, information about COG and EDG and how many personnel were in each of those two groups.

Second, even if that information was publicly available, because the defendant stole information from the CIA and gave it to WikiLeaks, who published information about it, you can find that that information still was closely held if the government took steps to protect it, which they did. That

information remained classified. Mr. Schulte only knew it because he was a CIA employee, who was governed by a secrecy agreement, that still required him to protect classified information.

Even after the leak, the government did not officially acknowledge or publicly recognize the validity of that information at the time that that email was sent. And in fact, you heard testimony from Special Agent Evanchec -- right -- that there was a search warrant that was filed. That search warrant is the subject matter of the email that Mr. Schulte sent to the reporter. That search warrant contained information that had been specifically declassified in order to be used in the search warrant.

Even after it was declassified, it continued to be protected, because it was only disclosed to the defendant under a protective order. And Special Agent Evanchec testified about that protective order. And Special Agent Schlessinger testified about that protective order. That's a court order that prohibits the defendant from disclosing the information outside of his defense team. So even though the information was declassified for a limited purpose, it remained closely protected and available lawfully only to the defendant.

Finally, you'll be asked to determine whether the defendant unlawfully transmitted that email to a person not entitled to receive it. And you should readily conclude that a

Washington Post reporter without a security clearance was not authorized to receive that email.

Finally, Count Four charges attempt to illegally transmit unlawfully possessed national defense documents in connection with the Malware of the Mind article and those tweets about Bartender. We've already discussed extensively why those two sets of writings contain national defense information: the advantages to adversaries that attributing particular cryptographic and cyber tool techniques to the CIA can have; and the risks of attribution from publicly connecting Bartender with another public report about another tool.

So the question you'll also be asked to decide is whether the defendant took a substantial step to transmit those things, and I submit to you there are any number of substantial steps that you can find from the evidence.

You can find a substantial step from the fact that Mr. Schulte wrote the article and that he wrote the tweets; from the fact that he redrafted and revised those tweets and revised the article; from the fact that he opened a Twitter account in order to be able to publish the tweets; and that he opened a Buffer account in order to be able to schedule tweets in advance. You can find it from the fact that he smuggled a contraband cell phone into prison in order to be able to open up all those accounts, those encrypted emails and those social media accounts. So you should readily be able to find that

there was a substantial step.

OK. So now we've walked through the charges and the issues that you'll be asked to decide in reaching your verdict. And you're almost to the end of me talking to you.

So you've been through, I think, about four weeks of trial at this point and you've been through a couple of hours of my summation, and in a few more minutes I'm going to sit down. And then after a break, you're going to hear from the defendant. And then after the defendant is finished, my colleague, Mr. Denton, will have an opportunity to speak to you for just a brief period. And then you'll receive your instructions from Judge Furman.

Before I leave you, I'm going to ask you to remember three things that Mr. Denton asked you to do at the beginning of this trial.

The first thing he asked you to do was to pay close attention to the evidence, and I think it is perfectly clear that you've been done that. Throughout this trial, you've been attentive and you've been attentive during my remarks to you. And I thank you and I appreciate it.

Second, he asked you to follow the judge's instructions on the law. I think it's also clear that you've been following instructions that Judge Furman's given you so far, and I know that you'll continue to faithfully follow his instructions during your deliberations.

Third, Mr. Denton asked you to use your common sense, the same common sense you use in your everyday lives. And now that you've paid close attention to the evidence and when you have heard Judge Furman's instructions on the law and when you apply your common sense, I submit to you that you will be led inescapably to one conclusion -- that the defendant is guilty of the charges with which he's been charged.

Thank you.

THE COURT: Thank you, Mr. Lockard.

All right. Ladies and gentlemen, as I said earlier, to ensure that you can pay careful attention to both sides, and since we've been at it for just under two hours -- I think that's close to the breaking point for listening attentively -- we're going to take a break now. So let's keep it to 30 minutes and then, as a reminder, we'll take another break of a similar length after Mr. Schulte before the government's rebuttal.

A quick couple quick but still important reminders.

Don't discuss the case. You haven't heard all the closings. You haven't heard my instructions. It's absolutely critical that you continue to keep an open mind until your deliberations begin -- really until you reach a verdict.

In addition, don't do any research about the case.

With that, it is 11:19, so let's be ready to go, if you can be ready for Ms. Smallman to retrieve you just a couple

minutes before 11:50 so that we can start promptly with Mr. Schulte's closing, I would be grateful.

With that, you are excused. Enjoy your break.

(Jury not present)

THE COURT: You may be seated.

All right. Anything to discuss before I give you your breaks?

Mr. Lockard.

MR. LOCKARD: No, your Honor.

THE COURT: Mr. Schulte.

MR. SCHULTE: No.

THE COURT: All right. Please be back in the courtroom ready to go at 11:45, and then we will start promptly with Mr. Schulte's closing when the jury is back. Enjoy your break.

Thank you.

(Recess)

THE COURT: You may be seated.

All right. Mr. Schulte, are you ready to proceed once the jury is back?

MR. SCHULTE: Yes.

THE COURT: All right. Very good. I will get the jury, and we will get going.

Are we ready to go?

MR. SCHULTE: Yeah.

THE COURT: I can't see it from here, but is that laptop in any danger of falling?

The jury is likely to be here any minute, so let's figure this out.

MR. SCHULTE: OK.

THE COURT: Good to go?

All right. Mr. Schulte, why don't you just take a seat, and then when the jury is seated and we're ready to go, I will invite you to stand.

(Jury present)

THE COURT: You may be seated.

All right. Welcome back, ladies and gentlemen. I hope you enjoyed your break. As I said before, I'd ask you to give the same careful and undivided attention to Mr. Schulte as he proceeds with his closing argument.

At this time, Mr. Schulte, you may proceed.

MR. SCHULTE: Ladies and gentlemen, Mr. Lockard is very worried about the lack of evidence, and you know that because he kept trying to tell you that the lack of evidence is not evidence of innocence. He's worried there was no forensic artifact of a log-in to the Confluence server. He's worried there was no forensic artifact of a copy command. And he's worried there was no forensic artifact of the transmission to WikiLeaks. And finally, he's worried there was no forensic artifact of any communication at all between me and WikiLeaks.

Well, ladies and gentlemen, he should be worried, because that is reasonable doubt.

It's still morning, so good morning, ladies and gentlemen of the jury.

Last time I spoke to you directly was three weeks ago, and I told you then I was not guilty of the crimes in this indictment. Three weeks later, that statement remains true. The government gave you no evidence, technical or otherwise, to convince you beyond a reasonable doubt that I'm the person who copied, exfiltrated, and transmitted the Vault 7 and Vault 8 information that ended up on WikiLeaks. And you know I was right to say that to you nearly a month ago.

The government, hand in hand with the CIA, has investigated this case for five years. Five years they investigated this case. We've had three weeks of testimony, nine witnesses, 1,200 exhibits, videos, audios, and several long slide shows.

What does all of this add up to?

I'll tell you what it does not add up to. The government still is not able to answer for you the very basic questions. In fact, curiously, I tell you there are more questions now than when the trial first began.

So for the next hour or so, I'm going to talk to you -- I'm going to try to be shorter here than the government has been. I'm going to review the evidence for you. I'm going

to try and cut to the chase, get in, get out, because it's been a long three weeks.

First, I'm going to look at how the CIA and the FBI together decided almost immediately that the person to look at, the person to focus on, the person to talk about, the only person to present to you was me. I'm going to talk to you about the government's motive theory. We'll dive through the forensics and what the evidence shows about the events at the CIA. Then we'll walk through the forensics from my home computers here in Manhattan. Then we'll briefly go through the DevLAN computer network, how it was the furthest thing from being secure, meaning that hundreds of people had access to it. Hundreds of people could have stolen it. Next we'll go through the charges at the MCC. And finally, we'll look at the charges and why the proof fails to support them. When we're finished, you will see that the only forensic, correct, proper, and fair verdict is a verdict of not guilty.

Now, as I talk, I'm going to flip through the slides on this PowerPoint. The PowerPoint will mainly display transcripts and exhibits that back my arguments. If you want, you can take down the exhibit numbers or transcript page numbers, but typically, I will move through the slides fairly quickly.

So let's begin with the crime.

On March 7, 2017, CIA documents show up on WikiLeaks.

This was front-page news, and until that date in 2017, the CIA had no idea that its crown jewels had been stolen. All they knew was that WikiLeaks was releasing their information and that more information was yet to come. The CIA was under pressure -- I will say tremendous pressure -- to find out what was leaked, how it was leaked, and who leaked it. They wanted to hold someone responsible for the leak, and so they began immediately an investigation, an investigation that focused on me.

The CIA joined up with the FBI, and literally, within 24 hours, they focused on me, the man who had left the CIA in November 2016 on bad terms. The lead FBI agent admitted that they had not even interviewed a single CIA witness. They had not even finished seizing the DevLAN network, let alone actually reviewed it. They had not conducted any investigation at all, and yet I was already the target of their investigation.

Then, within a week, the FBI concocted an impossible theory that the WikiLeaks crime occurred on March 7, 2016, because it was precisely a year before the leaks. That was a day when many other people were at a manager offsite and I was left alone in the office with no one to see what I was doing. And so the FBI argued I must have stolen the CIA's files.

The FBI swore out these false facts in a search warrant to a federal judge and then seized the 20 terabytes of

data from my Manhattan apartment. They scrutinized every device in my apartment, including even my Xbox, and ultimately came up empty-handed. The lead FBI agent testified that there was no classified information found on any of the electronics, there was no CIA backups or any CIA information in my home computers. No national defense information was ever recovered from my Manhattan apartment, and this fact is undisputed by the government.

Before we get into the forensics and technical evidence, let's just examine the government's theory of my motive to steal Vault 7 and Vault 8. I told you in the opening, and I tell you again now, the government's spite motive is pure fantasy. As the trial evidence has shown you, I've devoted my entire life, entire adult life, my work life to service. I started as an intern at the NSA and then at the CIA. Through my performance reviews and personnel files, you saw that I three years -- I went there as an intern, loved it so much I decided to graduate in four years instead of three. I was an award-winning developer.

But the government must come up with some motive. Right? So would do they come up with?

They come up with this story that they want you to think that as of April and May of 2016, I was boiling over with rage and anger. In fact, you heard Mr. Denton go on and on in his opening about anger, rage, spite, and revenge. And

basically they spent three weeks trying to show you that I was so angry with the CIA, so angry with management, that I decided to risk everything -- everything -- not only myself but everybody else and decided to risk the one country that I love by leaking this information.

But does this fit with what you learned about me throughout this trial?

The government did not ask a single witness if I was angry, not a single witness. FBI Agent Evanchec, the very first witness, even described my demeanor as polite, willing to answer questions and enjoyable to talk to.

Next, Anthony Leonis testified that he did not even recall my demeanor during the short meeting in which he issued me that memorandum.

Frank Stedman detailed one specific encounter with me in which he described me as casually annoyed.

Sean Roche, who claimed that I made a provocative statement and told him I could get my accesses back, even he described my demeanor as a normal, calm, conversational demeanor.

The government even played you videos of CIA security interviewing me. These were four-hour, grueling interviews, and the government selected few-minute clips from each. And what was my demeanor in those video clips?

You can play them again during deliberation. I was

laid back, calm, and collected. I'm an engineer. My entire job and life are based on logic. I may appear litigious and argumentative, but not angry.

Furthermore, Jeremy Weber told you that I was patriotic and that I was also antileaker. I thought Edward Snowden was a traitor who should be executed. He told you that I believed in the CIA's mission and thought nothing ever should be done against America, not ever.

You heard Mr. Denton tell you during the opening that I was nicknamed the nuclear option "because of my tendency to escalate and overreact when I felt aggrieved." He told you that I had a quest for revenge. Mr. Lockard just told you the same thing. But this is not even close to what the evidence shows.

Frank Stedman testified about my nickname, the nuclear option. And what did he say about it?

My colleagues used me when they didn't want to work on a project but didn't want to be the naysayer. I'm a very blunt person. The customer's idea is stupid, and I will tell them so. And we are not going to do it. Mr. Stedman told you I was the nuclear option because I skipped professional steps. I did not ask the customers how they feel or get all touchy-feely with them. I did not beat around the bush; I simply told them no. So my office used me in situations where this was necessary.

Nuclear option has nothing to do with overreaction or flying off the handle. In fact, what was Mr. Stedman's example of nuclear action? Do you recall what he said?

Mr. Stedman told you that I went to a meeting. Did I go crazy? No. Did I fly off the handle? No. At the meeting a customer asked how long will it take to write some specific code. Mr. Stedman told you that I pipe up from the back and say it will take months. And Mr. Stedman says, no, not months, but three weeks.

That is the definition of nuclear option. That is what the trial evidence has established. You can take a look at the transcripts and see it for yourselves. Nuclear option has nothing to do with escalation, overreaction, anger, revenge, spite, or any of that nonsense he told you in the opening. It is literally the opposite -- the absence of emotion and speaking bluntly.

All right. Let's briefly go through this motive timeline.

On March 1, 2016, I filed my complaint with security. The next day, TMU responds and sets a meeting for March 3. I meet with security on March 2 in which Amol denies the allegations and then admits them but claims it was all a joke. And at some point, Amol recants and an investigation kicks off.

Mr. Weber and Mr. Stedman told you they did not support me. That investigation continues for several months,

until security eventually concludes that there were no witnesses so the event cannot be corroborated or refuted.

At some point, I move from OSB to RDB. Contrary to the government's assertions, at no point do I consider this transfer a punishment or demotion. The email they cite was not an email asking if the removal -- let me rephrase.

The email they cite was an email asking if the removal from my previous branch was a punishment, not whether working in RDB was punishment. As both Leonis and Weber testified, RDB does great work and at this point in time employed many of the senior developers whom I had worked with before, when I was an intern.

The work done in RDB is a logical extension of the work done in OSB. RDB prepared tools for counterterrorism, as did OSB, except the tools in RDB were longer range tools. Trial evidence shows I was never once angry or upset at being in RDB. So that's it. As I told you in my opening, there was an unfortunate situation, and then I moved on. This move from OSB to RDB contributes nothing at all to motive.

Now, you heard Mr. Lockard tell you that I was planning to steal the backups starting as early as April 14, 2016. But of course, this makes no sense. As of April 14, 2016, trial evidence shows I still had access to the Confluence virtual machine. So if I were going to steal the backups, I could just copy them directly. I could literally log in to the

system and copy the backups, and I could do this on April 14 and April 15.

Mr. Lockard also told you I was casing the joint and deleted log files on April 16, 2016. Let's briefly take a look at what the expert said about those very log files that Mr. Lockard displayed to you.

Mr. Leedom told you this was normal activity. Mr. Leedom did not testify that there were any logs deleted here, and that is because this deletion is from a newly created file that was just uncompressed. After reviewing the uncompressed file, it is deleted, but the compressed log file still remains. It was never deleted.

MR. DENTON: Objection.

MR. SCHULTE: It's in the trial evidence.

THE COURT: All right.

Ladies and gentlemen, as I said to you this morning, what the parties argue in their summations is not evidence but their arguments as to what conclusions you should draw from the evidence. To the extent that your recollections of the evidence differ from theirs, it's your recollections that govern.

You may proceed, Mr. Schulte.

MR. SCHULTE: Mr. Lockard told you about googling hash algorithms, but of course, the experts testified that these searches were all relevant to my work at that time.

Mr. Berger testified that these searches were directly related to my work siphoning data. And take a look at what Mr. Berger says. Mr. Lockard spent substantial time talking about hash files and searches for hashing algorithms, yet all of this was clearly related to my work on CIA tool Nader.

What else did Mr. Lockard tell you?

That I stayed up late and locked up the vault in April 2016. But of course, the badge records show that I did this at least once every month.

Mr. Lockard then brings up the Google searches for WikiLeaks, but of course, as Agent Evanchec testified, there were multiple news events that occurred in the summer of 2016. WikiLeaks dumped the Clinton emails. Really? Come on. Everyone was reading that news -- Guccifer 2.0. The Shadow brokers released data, and even WikiLeaks claimed to have that code.

Mr. Lockard also brought up the diplomatic passport. Well, ask yourself, does Mr. Lockard's theory make sense?

By this time the CIA considers me a problem employee. I give notice of leaving the CIA. Do they have an exit protocol in place? Do they ask me? Isn't it equally plausible that both the CIA and I forgot about the diplomatic passport, a passport I never used? And why would I lie about a passport I never used? And isn't it just equally likely I left it in the office? And the trial evidence showed as soon as I realized

the mistake, the passport was turned over to the FBI.

OK. Back to the events at the CIA.

What happens next?

The OSB libraries.

You heard this story a thousand times throughout trial. Weber removed my accesses to the libraries, and then I undid his changes. This action was not performed secretly but openly. Mr. Weber testified that he did not recall whether I specifically told him I was adding my permissions back. Yet he just happened to perform a permissions audit and looked at the changes shortly after I confronted him. None of this really matters except what happens next.

The government wants you to believe that I committed crimes against my country because of a memorandum issued to me on April 18, 2016. Now, you heard the testimony of Mr. Leonis himself, and according to him, issuing a memorandum was very minor. It ranged very low in the hierarchy of potential discipline. It did not dock my pay. It did not put me on administrative leave. It did not reduce my grade. It did not even go into my personnel file.

Furthermore, Mr. Leonis told you that our meeting was very short. He issued the memo, I disagreed with it, he made some changes, I signed it, and then we moved on. A very short meeting and apparently not a very memorable one, because Mr. Leonis could not even recall my demeanor during the

meeting.

Like any other person, life gave me lemons. And what did I do? I made lemonade and went on with my life.

The sole consequence of the memorandum, the weekend removal all developers' administrative access, was something I had tried multiple times to relinquish to others. You heard Mr. Weber's testimony and saw documented, email proof that we had tried to transfer our administrative privileges to ISB since the very first day we took on those roles. It interfered with our real job. It was a favor asked of us, particularly asked of me, by the prior administrator. But it was something that I never wanted or cared about, and neither did Mr. Weber.

The events that transpired after April 20, 2016 are the most critical. These are events that occur after the government alleges I have already committed the crime -- events they cannot possibly contribute to motive. And these events show you that I did not commit the crimes alleged.

Now, just think about this. If someone commits this crime on April 20, 2016, what course of action would be the most logical?

They would have a goodbye party, say nice things and leave very soon after, on cordial terms. Or at the very least, you would keep your head down and a very low profile. You would not want to raise any alarms. Right? And what did I do?

Once I finished with development on Nader, I turned to

the second tool, a tool that the trial evidence supports I believed migrated with me to RDB -- Brutal Kangaroo. And then lo and behold, I discovered that I do not even have access to Brutal Kangaroo anymore. So I send an overt branch-wide email to ISB, at least ten people, requesting permissions for the project. After discovering that Jeremy Weber removed my accesses, I then sent an email to the chief, Anthony Leonis, and to HR about the issue. Not just once but twice. I send a follow-up email.

And then what happens?

Anthony Leonis tells me I should have surmised that he wanted me to pull out the subcomponent Shattered Assurance from Brutal Kangaroo. But you know that doesn't make sense. By this time, Shattered Assurance had been put to bed. And besides, the only way to do anything more on Shattered Assurance was by accessing the other subcomponent, Drifting Deadline, to which they claim I should not access.

My group chief then issues me a letter of warning. And do I keep my head down in a low profile?

Absolutely not. I complain to the group chief's boss, and then the group chief's boss's boss, Mr. Sean Roche. I filed complaints with everyone, including OIG. And then I find a job in New York and move here.

But most importantly, look at my course of action during this time and ask yourself this: Would someone who has

stolen from the CIA make himself such an obvious suspect? Would the leaker paint a big red target on his back? Of course not.

Finally, look at how I did things. I was litigious. I used formal process. I engaged with the Office of the Inspector General. I engaged with the Office of Equal Opportunity, EEO. Regardless if you think I handled the situation well or not, I think you have to agree that a person who leaked information to WikiLeaks in April 2016 never would have done any of these things. I used the CIA process to challenge my performance reviews. I wrote outside activity reports when I began talking to employment litigation law firms.

The CIA would not have any idea I was doing these things without reporting them, and these reports eventually led to those interviews with security that the government showed you. Those interviews only took place because I updated the CIA in accordance with CIA process and procedure. The result of these actions would only raise your profile following the leaks, which is precisely what happened. The real leaker would have either resigned immediately or simply kept a low profile. He would not have raised the Brutal Kangaroo issue with HR, and he certainly never would have escalated to the highest level of leadership at the CIA.

Now we've arrived at the first of many reasons why the

government's case is riddled with reasonable doubt: There is simply no motive here.

All right. Now let's talk about the forensics.

What evidence did the government's two forensic experts present to you?

The government knows -- the government knows -- that DevLAN and Altabackups were not secure and that many people could have taken the backups. So what does the government have to do to try and convince you about this supposed science, the technical computer evidence that they claim points to me and me alone?

If you look at the evidence, you'll see that it fails to support the government's case, and in fact, it supports the defense, just as I told you it would in the beginning. And a key witness on this point, as you remember, was the government's expert Mr. Leedom. He showed you a very long slide show about SSH keys, computer reversions, passwords, and many other things. Mr. Leedom ignored the insecurity of DevLAN and all the possible methods of extraction. He testified that he did not check any of the limitless possibilities himself or that he no longer remembers the results of those tests. And we'll get to those in a minute.

But, first, let's just focus on the tests Mr. Leedom did perform. He has clearly picked a team. The only logical inference one can draw from his forensic analysis is that

Confluence backup files were accessed on April 20, 2016.

Instead, what does Mr. Leedom do?

He asks you to take a giant leap without giving you the necessary technical platform. And there's where he loses his credibility. That is when he abandons the role of an expert and becomes an advocate. And you see this clearly on my first few questions of him on cross-examination.

Remember his forensic findings slide?

Take a look. What are the results of Mr. Leedom's forensic findings? Did he find a single forensic artifact that I even logged into the Confluence VM, let alone accessed or copied the backup files? Absolutely not.

Before we go into detail there, the government's theory rests entirely upon the predicate that the Altabackups directory was locked down. If the Altabackups were not locked down, which they clearly were not, as the evidence will show, then the snapshot-reversion theory is entirely irrelevant. If you can just open up this directory and copy the files, then you obviously do not need this complicated, convoluted snapshot-reversion theory.

And the government knows there's a gaping hole in their theory, so they try to quickly cover it up. According to Mr. Leedom, they know the access controls of all the directories and files on the CIA servers.

There, it shows the source controls and Gold

repositories that he testified about, the process of going through the security. And here, it tells you the permissions, who has access and what those accesses are. But somehow, magically, the government does not know what the access controls are to the Altabackups directory, the only one important for this case. Does that sound right to you?

Take a look again. Here is the directory, just like it exists in the Gold repositories. So why didn't Mr. Leedom just do the same forensic test to determine the access controls?

Because they would show there were no access controls at all. It is inconceivable that the government and Mr. Leedom cannot perform the same test and tell you the precise access controls for the Altabackups directory. Yet Mr. Leedom testified that I should go talk to ISB because, he claims, none of the access controls from April 2016 exist anymore.

And instead, what does Mr. Leedom do?

He relies upon an error message from the ESXi server and suggests that this error message definitively proves that there were access controls on the Altabackup directory. And then he makes another giant leap, without a shred of forensic evidence, and tells you those access controls must be super strict because that's the way he would set it up. But Mr. Leedom did not set up the access controls on the Altabackup directory. Mr. Leedom even testified that DevLAN security was

below average.

How can he possibly assume that the Altabackups directory was locked down, especially considering the lack of security mechanisms on DevLAN? And what was the reason for that error message from the ESXi server?

He told you I logged in to the ESXi server as a regular user, a user with no ability to run a mount command or perform any administration on the server, and then I run the mount command and it fails. Well, of course it fails. I did not have permission to run that command. So Mr. Leedom's giant leap of faith crumbles here.

Furthermore, there is significant testimony that the Altabackups were not locked down. You heard Mr. Weber's testimony about using the mount command in his own VM. If Mr. Weber can mount the Altabackups in his own VM, then they're not locked down at all. And even after the permissions change, you heard testimony from Dave. Dave was able to copy Stash backups and Confluence across the network. But after the permissions changed, there was only one Atlassian administrator, and it's not Dave. It's Tim.

So if there are all these access controls, how is Dave copying all these backups around?

But let's run with Mr. Leedom's baseless hypothetical that the Altabackups had some access controls. Mr. Leedom acknowledges that this error message does not indicate what

those are. Mr. Leedom also acknowledges that the Altabackup server is on a completely different subnetwork than the ESXi server. It's like a computer at your home trying to connect to a computer at your friend's home to download a file. There are many things that must be done to ensure connectivity across networks, and Mr. Leedom presents absolutely no evidence to you that the ESXi server was configured to access the Altabackup servers or mount any directories from that server. This is reasonable doubt in and of itself.

The government failed to prove to you that the Altabackups were ever protected; that there were any access controls at all on the Altabackups. Without access controls the potential suspect list is every single person who can connect to DevLAN, literally all 200 people. Everyone is a suspect, and most importantly, that snapshot reversion that he spent the majority of his time testifying about is completely irrelevant to the theft. The two are not related in the least.

So there was absolutely no need to execute a reversion to access the Altabackups directory, and this snapshot reversion is completely unrelated to the backups, but let's delve down into Mr. Leedom's theory and see how much more reasonable doubt we can find.

He claimed that the theft took place on a very specific date, April 20, 2016, and also gave you a very specific time. He said that I reverted Confluence back to

April 16 and stole the March 3, 2016, Confluence backup and reverted back to April 20. And specifically the time period between the two reversions is 5:35:37 p.m. to 6:51:17, an hour and 15 minutes.

Look at what Mr. Leedom says on cross-examination because that theory, I tell you, does not hold up. I asked Mr. Leedom a series of questions about whether he found any evidence of the copy command and instruction to copy the backups during the reversion period, and he admitted that he searched high and low for a copy command. I mean how else are you going to copy data without a copy command?

I asked him: You really looked, you looked for one, right? And he said: Yes, yes, I looked. And then he admitted that the government had asked him to look. The government wanted to find a copy command. He looked and he looked, and he never found any evidence of any copy command whatsoever. In fact, Mr. Leedom was able to review all the logs from my CIA workstation, because they were never deleted. He also found a transcript file from my virtual machine. And what do those transcript files say?

If there was a copy command or a log-in to the Confluence virtual machine, they would be right there.

(Continued on next page)

MR. SCHULTE: (Continuing) But there is no command ever executed. You see the last command that's executed, 21:29 is the result, and the very next command is at 21:55. And between that time, between 5:42 and 5:43, the Confluence backup files are accessed. If there is access or copy to that, those files, you would have seen them right in between these files, right in between these logs. These logs they have, they're completely in tact, if you go back. It is not missing any data, it is all complete and in one file. So what you would expect to see are these commands in between here. This is the time period when the backup files are accessed. So you would expect to see, as Mr. Leedom said, these commands which he never found, or he testified that would see a command to do the copy.

So how could I have possibly copied any files without executing a copy command? This has absolutely nothing to do with any deleted log files from the ESXi server. As I told you in my opening, the government is trying to distract you with these unrelated deleted files. In fact, Mr. Leedom himself admitted that there would be no copy command log in those files. The reversion from Confluence also could not have affected the log files from my CIA work station. If I had copied the backups, the logs would be stored right on my computer.

But, most importantly, he has the logs from my

computer, the computer I am using to access the ESXi server and other servers. Everything I do, every command I run from my computer is logged right here. He has all of those logs and admits those logs were never deleted. So where is it? Where is the copy command? If I didn't copy the backups then there would not be a copy command, right? And there is no copy command. So obviously I did not copy the backups. The missing copy command is yet more reasonable doubt.

Next Mr. Leedom testified that he recovered all of the removable media I used at the CIA, yet he found that none of it contained forensic evidence of the backups. In fact, the logs from my CIA computer definitively show that no devices were ever connected during the reversion period. No storage device. No thumb drive. No removal of hard drive. No drive. Nothing. Nothing that was ever connected to my work station computer during the reversion period. Nothing is plugged in. What am I copying the backups to without a device connected to my computer? Well, there are countless logs and other activities that Windows records that would alert the forensic examiner that the backups were copied right to my computer. And anyway, the backups would have been copied onto some device for it to make -- let me rephrase that. And anyway, the backups would have to be copied onto some device to make it outside of the CIA. So what is the government's theory? To what device are the backups copied? They never tell you. They never tell me.

They still do not have a theory. That, ladies and gentlemen, is the very definition of reasonable doubt, when the government has no clue and cannot pose to you a theory based upon even circumstantial evidence, then that, alone, requires acquittal.

Next Mr. Leedom does not even present to you, with any forensic evidence, for whether those files could even be copied in the time frame of the reversion.

After the final reversion back to April 20th, 2016, at 6:51:17 p.m., that cannot even access the Confluence VM anymore. The copy must finish in this time frame. Yet, because he has no theory as to what device the data is copied to, he cannot possibly give an estimation for the amount of time the copy will take. It depends upon how fast the device is. It also depends upon the network speed. According to the size of the backups, that's at least 200 gigabytes, about 1,000 episodes of Netflix. And all in an hour and 15 minutes? You can do the math. Is that possible? I mean when you need to download 200 gigabytes from the Internet, can you do it in 75 minutes?

Think about it. How long does it take to download files onto your computer. And does Mr. Leedom establish that the DevLAN network is faster than the Internet? Does he establish any bandwidth for DevLAN at all? No. He does not even have a slide about it. He does not even want to talk about it. The government very quickly just asks him if it were

possible and he said yes, without presenting to you evidence or even a slide illustrating the speed of DevLAN. The government has failed to prove that the backups could be copied in the short window. Ladies and gentlemen, once again, this failure establishes reasonable doubt.

And that's not all. There is yet another major problem with the government's theory. During the time when the Altabackups are accessed, 5:42 to 5:43, the trial evidence shows I'm not in the vault or at my computer. According to the badge records I tried to badge into the vault at 5:45 from an access point near the mens bathroom, according to Mr. Weber's testimony. I mean, take a look at this. If I am badging in from the bathroom at 5:45, at 5:42 and 5:43 I'm in the bathroom, I wouldn't even be at my computer. It is just not possible that I ever accessed, let alone copied, the backup files. Ladies and gentlemen, once again, you have reasonable doubt.

Finally, there is one remaining, very significant forensic finding here. Mr. Leedom told you that those transcript files from my CIA computer were not normal. Normally you only see the input of commands but not the output, yet he found transcript files from my computer showing both input and output. These are the activities that show the deletion of log files from the ESXi server. He admitted to you that he has absolutely no idea how these files were generated

but he agreed that they could be generated through user intervention. He also agreed that system administrators will record their actions on a system to preserve activity logs. Then, if something happens, you can review what another administrator did. Mr. Leedom offers you no other explanation for these files. None. The trial evidence should make it clear to you that I must have generated those files.

The trial evidence makes clear that the generation of these files requires user intervention, it requires the purposeful intent by the user to record his session and all commands executed thereafter. And the trial evidence also makes clear that recording sessions transcripts is in accordance with system administration best practices. If something abnormal occurs, such as deleting log files, a record of it should be kept so that when other administrators log in, they are not baffled by the missing logs or other abnormal activity. They can review the transcripts and see what happened, that's the point of transcript files, to record abnormal activity. And this requires direct user intervention, you have to take deliberate, purposeful action to treat these files.

So now think to yourselves, would someone purposefully record themselves committing a crime? Generating transcript files to record yourself committing a crime is a forensic equivalent of installing a security camera and setting it to

record in a store before you rob it. Does that make any sense to you? Based upon the existence of these files, you should infer that I purposefully recorded them and was not doing anything malicious or illegal. The very existence of these transcript files establishes reasonable doubt. And this is even confirmed when you look at Mr. Leedom's slides.

If someone were trying to cover their tracks, they would just delete logs at the very end after they were finished doing whatever malicious act they were doing but you don't see that here. Here you see a very methodical method is followed. You see deletions throughout this hour at regular intervals, specifically the first and the last occur within two minutes, and in between it is every 20 minutes. You see a check of log files, then a deletion, and then 20 minutes later the same exact thing; a process that is being followed here, a technical procedure, and not malicious activity.

As I told you during my opening statements, the government's own forensic experts have proven my innocence or at the very least their experts have left you with insurmountable reasonable doubt. Mr. Leedom's testimony is devastating to the government's case. Think about this: The government cannot establish the four core steps necessary to commit this crime. And what are those steps? Access -- you need access to the information such as a login to the Confluence virtual machine. OK? You need a disk, a disk drive

or some mechanism to store the data you want to steal, inserted it in the drive, and the copy command. Files cannot copy by themselves, you need a copy command.

Exfiltration. You need some way to take the data out once you have made a copy. If there is no login to the Confluence VM during the reversion period, no copy command, no removal drive connected to my computer and no network speed established to tell you how long such a copy would take. And, I never took any devices out of the CIA. And, I was actually in the bathroom during the access to the backups. I could not have stolen that information and if I couldn't have stolen that information I certainly couldn't have sent it to anyone, let alone WikiLeaks. And one of these failures establishes -- any one of these failures establishes reasonable doubt and a combination of all of these establishes that the government's theory isn't just doubtful, it is impossible.

Is Mr. Denton able to tell you how I copied the Altabackup files without leaving a copy command anywhere? No. And because he can't, he falls back on the "because you deleted it" argument. He never explains how I download all of those files without connecting any device, any thumb drive, hard drive, anything to my computer. He never tells you how it is possible to download 200 gigabytes in an hour, how I copy filed from the bathrooms, how I take this non-existent device out of the CIA without anybody noticing. There were armed guards.

You have to badge in, badge out, sit in a vault, sit in a safe. How do I get it out?

Now let's move on from Mr. Leedom and the CIA to my Manhattan apartment and Mr. Berger. And recall the first witness, FBI Agent Evanchec who testified that none of the files on my home computer, including the encrypted containers had any classified information on them. So what did Mr. Berger offer you? Mr. Berger confirmed these results. Mr. Berger also testified extensively about certain activities in April and May 2016 like Google searches and Amazon purchases, but for a computer geek like me, like I told you in my opening, this activity is consistent with my habits and hobbies.

MR. DENTON: Objection.

THE COURT: Ladies and gentlemen, a reminder that what Mr. Schulte is saying in his closing, everything he has said during this trial is not evidence. You can consider it as argument but not as evidence and in that regard, with that, you should listen to what his argument is.

You may proceed, Mr. Schulte.

MR. SCHULTE: As the trial evidence showed and you are about to see, there is literally nothing unique about the activities in April and May 2016.

While Mr. Leedom worked as a contractor for the FBI, Mr. Berger is the FBI. It is clear what team he has chosen. Mr. Berger deliberately omits evidence, demonstrating that my

activity is normal during this time, he zooms in on details, cherry-picks data points and insinuates to you that certain activity is nefarious or suspicious. In essence, what Mr. Berger has done is zoom in and ignore the big picture.

Take a look at this example. It looks like a straight line, right? But that is zoomed in at 2,000 percent. When you zoom out, you see that it is a circle, a shape composed of absolutely zero straight lines. Appearances can be deceiving. This is what the government, and particularly Mr. Berger, has tried to do to you -- zoom in and ignore everything else. Zoom in and focus on a few Google searches while ignoring my full Google search history. Zoom in and focus on a single device I purchased while ignoring my full Amazon purchase history. Zoom in and focus on activity of a certain night while ignoring the surrounding 1,000 days that formed my habits. At the end of the day you just have to ask yourselves, isn't their bias skewing their investigation? Why obfuscate? Why not provide full context? Why not function as an expert instead of an FBI agent and advocate for the government?

Mr. Berger testified that I transmitted CIA backups to WikiLeaks. Let's see. And what is the basis for that conclusion? Google searches. They really should be renamed the Federal Bureau of Google because their entire forensic analysis consistently starts and ends with Google searches. And of course this slide that Mr. Berger presented to you, no

evidence that anything was ever transmitted to WikiLeaks, it does not even give you a theory as to when or how this occurred.

Mr. Berger starts with the WikiLeaks website. He showed you what it looks like in April 2016, but recall FBI Agent Evanchec's Google search analysis. I never visited the WikiLeaks website in April or May of 2016. I could not have possibly even seen the WikiLeaks site. But, of course, when the Google searches don't mesh with the conclusions the FBG wants you to draw, then they ignore the Google searches.

Mr. Berger tries to insinuate that I must have visited the WikiLeaks website because I downloaded Tails even though the forensics shows I consistently downloaded Tails and other Linux distributions. There is literally nothing special about Tails. There is nothing in evidence that distinguishes Tails from any other live boot Linux distribution.

Mr. Berger then tries to make something special out of TOR on a virtual machine. Mr. Berger fails to establish that the VM was even installed on my home computer or even used by me but regardless, the forensics show that the VM and TOR were installed and used back in 2015. Again, this is typical activity throughout this time.

Next Mr. Berger talks about the purchase of a SATA adapter. Only, it is not a SATA adapter, it is a hard drive docking station. Its primary function is an offline clone to

make complete copies of other hard drives. It cannot be connected to the Internet, it is not used to transfer data, and I would not need it to connect hard drives to my computer since I have fast eSATA ports on the back. Not only that, but I buy the same device several months later.

Let's talk about these other devices that Mr. Berger does not even mention. 118, you see a hidden camera in a pen that is purchased; multiple hard drives; all kinds of digital devices are purchased throughout this period. My purchase history shows this activity is normal, it is consistent with my habits and my hobbies.

Mr. Berger then talked about Eraser Portable -- and I'm not really sure why -- securely deleting a folder labeled Array List, and as he confirmed, which is a basic data structure taught in entry-level programming classes. Securely deleting this shows that I was simply testing Eraser Portable.

And as for Brutal Kangaroo, you heard Mr. Weber tell you that we worked on projects outside and then brought them into the CIA. Brutal Kangaroo was a project I was working on at this time and, as Mr. Weber told you, sometimes source code can be linked to individuals. So after taking source code into the CIA, it would be prudent to erase that code afterwards. And, of course, as Mr. Weber told you, tool names are unclassified. So there was absolutely nothing improper with having a folder named Brutal Kangaroo at my house and nothing

improper with writing code and bringing it into the CIA.

Mr. Berger then identifies for you a particular night, April 30th, 2016 to May 1, 2016, and he identifies this night because of late Google searches and logins to a virtual machine. But of course what he fails to tell you is that the forensic evidence shows I was up late playing League of Legends. In fact, the forensic evidence showed I often stayed up late playing games. This is not uncommon, but he zooms in to this specific night and ignores all other days.

Mr. Berger also talks about wiping and reformatting. He claims that I wiped my computer on May 5, 2016, and reformatted it. But, of course, that isn't true at all. When installing a RAID 5 system, it automatically formats the drive such that each file is essentially split equally across all three drives. And the forensics clearly support that I upgraded my home computer. I installed a RAID 5. The new RAID installation explains everything. It explains the Google searches, the data transfer, the docking station to clone hard drives and the use of DBAN and other disk wiping utilities. You don't want to keep your financial and personal data sitting around on loose drives. It is common best-practice security to wipe those drives.

So what is Mr. Berger's theory about the transfer of data to WikiLeaks? He doesn't really have much of a theory except to speculate a time frame between April 20th and May

5th. But even for that theory he doesn't give you any forensics, any forensic evidence.

Once again, Mr. Berger slips off his expert witness hat and flips on his FBI government advocate badge. Mr. Berger's forensic findings that there is absolutely no evidence at all that I ever contacted or transmitted any data to WikiLeaks establishes even more reasonable doubt.

Finally, it is important to talk about NetFlow logs. 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 --

MR. DENTON: Objection.

THE COURT: Sustained. Sustained.

Please stick to the evidence, Mr. Schulte.

MR. SCHULTE: Mr. Leedom:

Question: Can you explain for the jury what NetFlow logs are?

Answer: It is essentially like, a summary of, bytes in and out of a network. So, theoretically, if you had NetFlow logs you could determine between two points in time how much data transferred from one point to another.

So from the NetFlow logs you can determine basically the amount of data sent or received by each connection, correct?

Yes.

Which would have been very huge in your incident response, correct?

Yes. It was one of the first things I asked for when we showed up.

And as for Mr. Berger the question was: NetFlow logs would establish definitively whether or not data was transmitted or received during this time period, correct?

He responded: If, depending on the records they would establish what data was transferred or received over the connection from Verizon, then yes.

So this data can irrefutably link you to every single data transfer you perform. Even if you use TOR or other proxies, an anonymizer, your Internet provider will still capture the fact --

MR. DENTON: Objection.

MR. SCHULTE: It is in the record.

THE COURT: Ladies and gentlemen, I think you understand at this point that what Mr. Schulte is arguing is his argument that is not evidence and in that regard you should rely only on the evidence and the conclusions that you draw from it. With that in mind, please listen to Mr. Schulte.

Go ahead.

MR. SCHULTE: Your Internet provider will still capture the fact that you transferred data across it. Mr. Leedom testified about the importance of NetFlow logs.

This was the first thing he asked for. If DevLAN had kept these logs then we would not be here today. The data would definitively unmask the two perpetrators. Unfortunately, no such logs exist on DevLAN. However, Verizon did record those logs from my home connection. Verizon provided the NetFlow logs to the government. The government reviewed those NetFlow logs and provided them to me. The government then stipulated to the accuracy and admissibility here at trial under stipulation GX- 3006; you have them, Defendant's Exhibit 208. We even went through the data with Mr. Berger, it is a big spreadsheet. And through Mr. Berger we cut it down to this time frame between April 20th and May 6th, and that's marked as Defendant's Exhibit 208-A.

Since the government cannot establish any connection to WikiLeaks or transfers of 200 gigabytes in this time frame you can only infer that neither occurred. Here is the data, here I am on trial. Those NetFlow logs, according to their experts, would show if I sent a byte of data to WikiLeaks. And the government, five years later, never pointed you to any of that data. The government did not even seek to introduce it but both the existence of these logs and the government's failure to direct you to any transmissions to WikiLeaks or transmissions of 200 gigabytes of data during this time frame raises significant reasonable doubt.

Let's take a minute to go through the timing analysis

for the Vault 7 and 8 release by WikiLeaks.

Both experts testified about this to varying degrees. The point is version control which existed in both Stash and Confluence and keeps track of all iterations for each file. Every time you modify a file, that changed the file that saved. And what this means is every successive backup contains all the data from all preceding backups. March 4th contains the day from March 3rd, plus the new changes. So it is really trivial to go through the data and select files from a particular date. So while the experts tell you it has to be the March 3rd, 2016 backup given to WikiLeaks, this is simply not true. They are not testifying as experts at this point but as FBI agents, advocates for the government. No forensic expert could testify as to what files WikiLeaks received, they simply have no idea. The forensics can only establish one thing, what is 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.

But, the reverse is not true. A new backup can and does contain old files, this is why upper bound can be

established. If you have files from March 4th, they can 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 3rd, 2016. The data released by WikiLeaks could originate from each and every backup from March 3rd, 2016 to March 6, 2017.

I also want to talk to you just for a few seconds about the document that the government keeps showing you, OK; 1207-27, 1207-30. The document that indicates that March 3rd, 2016 Confluence backup was accessed on April 20th, 2016. That doesn't show it copied. I don't know how many times they showed it to you. I think they showed it to every witness they could find. You know, we could have made this whole process more fun by turning it into a drinking game when you take a shot each time the government shows you 1207-27, although I don't think you would be able to walk by the end of the day.

Let's just take a look at 1207-27 because what this document does not tell you, it simply does not tell you who or which work station is doing the accessing. It doesn't tell you that. And you know they tried to fill that gap because David Denton, in his opening statements, tried to get you to think that March 3rd somehow had some significance to me and that is why March 3rd was picked. But Mr. Lockard did not even try to explain why, on April 20th, a March 3rd backup is being taken.

Why isn't the April 20th backup taken?

There is nothing in the evidence to support any claims that there was any significance at all to March 3rd because I never mentioned this date. There is no evidence of me mentioning this date. The only people who somehow think March 3rd is an important date are the prosecutors because it is their mission to convict me.

Second -- and every single witness tells you this -- access, again, is not the same thing as copying. Just remember what the government's own witnesses told you, that the April 20 timestamp -- I remember they told you this, it stood out like a giant red flag -- because it is the only entry where the numbers in the right column do not match the numbers in the left column. Right?

So think about it. I am a trained expert in stealing computer information without leaving a trace, right? That was literally my job. It is a job for which I won awards. I even wrote about it in the notebooks at MCC. Why would I leave such an obvious red flag? You heard testimony that access times are changed by a single command, a touch command. Do you think the CIA malware I write leaves time stamps like this when it steals data from adversaries? I wouldn't have a job for very long if it did.

Go back to Mr. Leedom again. Remember when I asked him if he ever heard of something called a touch command? And

he said a touch command is a command in Linux, it is a command you can use to change file access times; a very short, easy command to run. And he agreed with me that malware sometimes, what he called, time stomps files. Do you remember that? He explained that malicious actors time stomp files when cleaning up their activities to mask the fact that they accessed or edited a file.

And you know from Jeremy Weber that I was an expert in Linux and system administration. Whenever the individual who set up the Atlassian project leaves for an overseas assignment who does he go to for help? Out of all the developers at the CIA he came to me. So if I am really going to be stealing the data on April 20th and all I have to do is use a simple touch command to change the April 20 access time back to March 3rd, 2016, I could have, and it would have looked just like this. That's your touch command. Look at the day now. That's a simple touch command, it would have looked just like this. The timestamp on the right column would have matched the timestamp on the left column with a simple touch command.

THE COURT: Ladies and gentlemen, I think it is clear from the slide itself but that is a modification of evidence that is in the record just intended for argument and demonstration purposes. That obviously is not in evidence itself.

MR. SCHULTE: So why would I leave such a giant red

flag like this for investigators to find? You know I wouldn't have, and that's how you know it wasn't me who committed these crimes. And I want to take a minute here to point out a fundamental contradiction in the government's theory when it suits them. When it suits them, they want you to think of me as this careful, genius, cyber criminal who can cover up his tracks at-will, and then there are other times when I am so inept and such a bumbling data stealer that I am hunting in the ESXi server looking in the wrong place and that's why I can't find and delete VIclient files. So which one is it? Which one is it? Because you can't be both, right?

And do not for a minute believe that they have any evidence that this information went directly from the CIA to WikiLeaks. They have never proven that to you and they have never explained again why the March 3rd, 2016 backup file on April 20th, 2016. Nor have they explained why WikiLeaks, a news organization who wants to publish leaked materials, why they would wait a full year to release this information. It makes no sense. It is far likelier that WikiLeaks received this data at the end of 2016 into 2017. And maybe Mr. Denton will also explain to you why WikiLeaks waited almost a year and not a week, like Mr. Leedom took, to discombobulate the information. A year. Why would WikiLeaks wait a whole year to release this information? We will have to wait and see what he says.

Before moving on, I just want to remind you that it is up to you how much credence you give to each witness and you should be careful in reviewing the government's tech expert's testimony. On one hand they presented you technical evidence and on the other they testified as FBI agents; Berger worked directly with the FBI and Leedom was an FBI contractor. The government did not go to the private sector and ask an independent forensic analyst to conduct a review, they asked one of their own to conduct a review. In fact, think of the difference in their demeanor on direct versus cross. When the questioning got tough, how did those experts react? They don't know, they just do what they're told. That's not the role of an expert analyst. They don't sit around and take direction from the government and make conclusions the government pays them to make. A forensic analyst is supposed to take the initiative to perform all tests and analyses required, to set out and test the hypotheses and document each step so another scientist can confirm their result. But, of course, that didn't happen here. They work for the government so there is substantial bias in their testimony and you can tell when they crossed the line when they present you with facts, forensic artifacts and testable hypotheses, they are functioning as experts. But when they start speculating and they ask you to take giant leaps without laying any technical foundation, when they start making baseless conclusions, then they are

functioning as FBI agents and advocates for the government.

There are several examples of this that you have already heard. Mr. Leedom's expert presentation included a slide of his forensic findings that we already went through in which he concludes the March 3rd, 2016 Confluence backup file was accessed, not copied or accessed by me. These are forensic findings he made as an expert witness. However, when he states belief that I am guilty, that's the testimony of an FBI government advocate. The same with Mr. Berger. Although Mr. Berger admits there are no forensic artifacts and not a shred of evidence, forensic or otherwise, that I ever transmitted anything to WikiLeaks, he states his belief that I am guilty.

Again, this is testimony of an FBI government advocate, not an forensic expert, so when reviewing the expert testimony you should look for what the basis is for the testimony. Is there forensic data references? Forensic artifacts? A repeatable test? If not, then you should ignore their testimony.

So you might be asking yourself now, OK, if it wasn't you, then who was it? I just want to take a minute to remind you it is not our job to solve this puzzle. It is not our job to solve this crime. It is not my job and it is certainly not your job, that's the government's job. We are not the FBI, we are not in the business of accusing, we do not bear the burden

of indicting and proof. So what did the government's investigation uncover?

The FBI learned from working with the CIA, day in and day out over a period of five years, that the CIA's DevLAN network was highly insecure; there were no access controls, there were no user controls, user shared passwords, passwords were weak, passwords were stored openly, there were no audit logs, there were no login activity checks, anyone could connect their DevLAN work station computer to the Internet just by taking the cable from one computer and plugging it into the other. I mean, think about how crazy this is. You just swap out the cables in the back and instantly all the classified information is connected to the Internet. It could be transmitted without leaving your desk.

You have Dave making all these copies of Stash and Confluence and storing them in public locations. Do you recall that? The OSB test repo and a live Confluence system, no access controls. Dave even loses a hard drive with a copy of Stash. You know, there is simply no accountability.

Special Agent Evanchec told you that nearly every witness he interviewed described DevLAN as the wild, wild west. Why? Why use that phrase? Because it tells you the system is not locked down. Nearly ever CIA witness told you this. You know that people on DevLAN shared passwords and not only do they share passwords, they were extremely weak and simple

passwords. What does that do? It made it impossible to account for who was using the password and, again, it left the system vulnerable.

Take a look at the WikiLeaks task force report GX- 5001. They tell you, they confess and they say we cannot determine the precise scope of the loss because DevLAN did not require user activity monitoring or other safeguards that exist on our enterprise system. These are not the defense's words, these are the words of the CIA. Day-to-day security practice had become woefully lax. Most of our sensitive cyber weapons were not compartmented. CIA admits the user share system administrative level passwords. There were no effective removable media controls. And, historical data was available to users in definitely. This is all in their exhibit. It goes on to tell you the stolen data resided on a mission system that lacked user activity monitoring, it lacked a robust server audit capability. And then it says the CIA did not realize the loss had occurred until a year later when WikiLeaks publicly announced it in March of 2017. Had the data been stolen for the benefit of a state adversary and not published, we, the CIA, would still be unaware of the loss.

So why is this important? The bottom line is this: Because the system was insecure, because the system was poorly monitored, the government cannot know and it certainly cannot prove to you which of the many people with access to this

information committed this crime, when they committed it, or how they did it. And they haven't even touched upon foreign adversaries, nation states, non-state actors, they haven't even touched upon any of that.

Think about it this way. It is like your home. If hundreds of people have a key to your home, if you leave the door open, if you leave your windows open, you always leave your door and your windows open and unlocked, can anyone just come in and at any time that they want, take your stuff, walk out with it, and you would never know it was gone until you needled to use it again. You wouldn't know who stole something from your house if you left your house that unlocked. And you know who else doesn't know? The CIA doesn't know.

And it wasn't just DevLAN in general that we are talking about that was insecure. We already went through the access controls on Altabackup. Mr. Leedom claims those access controls were lost, he has no idea what they were, but based on the set of security on DevLAN it should be clear that there were many ways to -- the backups. So if DevLAN and Altabackups are not properly protected, what does that mean to you? You already know this because you have been here with me for three weeks. You know what it means. It means that all 200 people on DevLAN had access and could have committed this crime. If that many people had the access and ability to commit the crime, that is reasonable doubt. And even if there were access

controls, who were the people who used DevLAN? They were all trained CIA hackers with access to all the malware they've ever developed at their fingerprints. These are people trained to steal data without leaving a trace. This is CIA malware that cannot even be detected by anti virus software, malware that cannot be identified by people like Mr. Leedom who are trained forensic examiners. Even if there were any access controls on DevLAN or any of the other data, you would just need to pull off malware that has already been written, software that's been around for years, and then run that malware on DevLAN to exploit it and take what you want.

So once again, since all 200 people on DevLAN had access to malware that could break into DevLAN itself and the ability to commit the crime, that is reasonable doubt.

Let's not forget that there are spies working for other countries who are trained to do exactly the same thing. We are not the only people who have a monopoly on this skill set. And the other side can do to the CIA exactly what the CIA does to them. This is just common sense. Foreign intelligence services want access to classified U.S. computer systems and documents just as the CIA wants access to classified documents from other countries. There were also venerabilities outside DevLAN itself. Let's take a look at the offsite backup.

The offsite backup is a storage location outside of the CCI office that contains all the data from DevLAN. The

government mostly ignored the offsite backup. Neither expert has even been to the site and they provided zero forensic evidence from the offsite backup in their presentations. What was the process for transmitting this data to the offsite backup? Was it electronically? Was it hand-carried? Was it exploitable? The government gave you no evidence. Who has access to this DevLAN data from the offsite backup? What are the access controls there? How many people have access? The government never says. Why couldn't WikiLeaks receive a copy of the data from this site? It is the same data.

Let's talk about the Hickok Jira connection. Again, the government completely ignores this but EDG's DevLAN network is connected to COG's network through Hickok, and Jira sits on Hickok and Jira mounts the Altabackups. So, someone from EDG or COG just needs to access Jira and they can access all the CIA backups to the Altabackups. Did the government even conduct an investigation into Hickok or the COG network? They did not. Neither expert knew anything about Jira, Hickok, or COG. Neither expert had reviewed or accessed any of those networks.

The government either did not even conduct a full investigation or chose not to call the witnesses who did. I mean, think about this. It would be just one slide -- one slide -- with the access times of the backups from the offsite backup, one slide detailing the security of these other

networks and why it could not have come from them instead of the Altabackups, but these experts the government showed you didn't even conduct investigations into these sites. So who did? Did anyone? You have no idea. I have no idea. If someone hacked the servers at the offsite backup site and sold the backups from there, how would the government know? If someone from COG hacked the Jira server, accessed DevLAN and stole the backups how would the government know?

These are not crazy speculative theories, these are the first steps in an investigation. Step one, how many places contained the data released by WikiLeaks? Step two, who had access to these places? Step three, what were the securities policies? Step four, forensic examination. Once you eliminate a site you go to the next one. These experts all testified that the data must come from DevLAN, specifically to Altabackup, but why? What is their basis for that determination? If they testify -- they testified they never even reviewed the other sites so how can they make such a conclusion?

The government does not have a shred of proof for any of these espionage charges. So what do they give you? They focus over and over and over again on the MCC evidence and they focus on my writings. And they seem to think that these writings will take the place of actual proof of theft on the WikiLeaks charges. But these prison charges are the equivalent

of the sacrificial bunt in baseball. The government knows they have no chance to convict on these charges but they use the MCC counts to present you with private personal prison notebooks and statements I wrote therein. The whole point is to show you videos of me in prison to humiliate me, vilify me, dirty me up and make me seem like a bad person.

Now, if you were falsely accused of a crime and incarcerated for years pretrial, isolated from your families, friends, and life itself, you may have acted differently. But I'm not accused of smuggling cell phones into MCC, of using cell phones at MCC, of using drugs at MCC, or anything like that. I'm accused of transmitting national defense information from prison. And you will soon see how absurd these allegations are and recognize the sacrificial bunt as the dirty play that it is, a way for the government to kick a man while he is down.

MR. DENTON: Objection.

THE COURT: Sustained.

MR. SCHULTE: So what kicked off the event that the led to the MCC charges?

The evidence shows you that there are many cell phones in the MCC. Mr. Betances told you that I went and exchanged an iPhone for an Android with another inmate. Cell phones abound. They are everywhere at the MCC. But when the government learns that I have access to a cell phone from the MCC, what do they

do? They shut down the MCC and send in 50 trained FBI agents to find that cell phone. And why do they do this? United States government is terrified of the highly sensitive national defense information that I retain in my head. I worked for the NSA and the CIA for years developing, testing, and assisting in the deployment of cyber operations around the world. I have, to this very second, knowledge and information that can cause substantial damage to the United States. Had I wanted to harm the United States isn't that the information that I would set loose into the world? Isn't that the information that I would threaten to post on Twitter? Isn't that the information that I would e-mail Shane Harris? But in the hundreds of pictures and videos taken by Mr. Betances, there was not a single classified document or any illegal activity at all aside from the cell phone itself.

In the government's shakedown what do they uncover? What did those 50 FBI agents find? What was I doing with cell phones at the MCC? More of the same. I was drafting articles critical of the criminal justice system. I was fighting my case, the charges against me. Evidence will show, through the notebooks and evidence collected through electronic search warrants and subpoenas, that I viewed my incarceration in a federal prison just like any convicted inmate, to be an egregious violation of that social contract created and signed by Convention in 1787.

So let's look at what I sent Shane Harris. I sent him a copy of the government's search warrant. Why? What is this trial going to show you? I was trying to get him to write about my innocence. I wanted his help, his audience, his reach. I wanted to prove my innocence. Remember, by now, I had been in jail for over a year already.

So let's look at these writings. You have them in evidence. I am clearly deteriorating at this point. Prison is not a nice place. It is not a place that anybody wants to be so compare, compare my prison writings to the way I write at the CIA and you can see I am coming apart. In fact, you can see multiple times where I am talking about using drugs in the notebooks, particularly when you see what the government references as draft Tweets. The evidence shows that these are not reel Tweets or even planned Tweets, this is a re-counting of a man's hallucinations.

What does the government want you to believe about these writings? The government wants you to believe this is some kind of planned army-like information war against the United States. Just compare what the United States wants you to think about as this information war and what the information war actually is.

Let's just take a look at the titles: Presumption of Innocence. A Petition for Redress of Grievances. A Loss of Citizenship. Do You Want to Play A Game? Detention is not

Punishment. Guilty Until Proven Wealthy. Can You Afford To Be Accused. A Proposed Solution Origin. Does this sound like a battle plan? Is this what he called a battle plan?

So what did the trial evidence actually tell you about the MCC conduct? My focus here is not about anything other than trying to prove that I am an innocent man sitting in jail. That's what the plan is, right? I want to get out because I am innocent. I want a chance to fight my case from outside, to be with my family. So what do I do? Yes, I use a cell phone, a cell phone that was smuggled in, and I used it to try and get my story of innocence out to the Washington Post. I tried to get it to the Washington Post and to anybody else who will listen. And that is what I do with the search warrants. I write out why I believe the search warrants are false and that is what I am trying to get out.

And look, I'm not going to stand here and tell you that using a cell phone in a prison is right. It's not, it's against the rules. Did I use a cell phone? Yes, but that's not what I am charged with. I am charged with far more serious crimes here and they have no proof I committed those crimes which is why they're so focused on the MCC conduct. They want you to focus on the MCC conduct because that is the only way they think they can get you to believe I committed the WikiLeaks offenses.

Just for a moment, take a look at what I say. Take a

look at what I say in these articles and just for a moment take a look at Malware of the Mind. See if this is what you would have in your head if you are trying to betray your country. What does it say? Today we are facing a stealth constitutional crisis. A Malware of the Mind has entered and corrupted the justice system.

What am I talking about? I am talking about the justice system. Again, from there I go on to talk about the justice system in the context of technology, how the law does or does not progress with technology and how these prosecutors and FBI agents, with very little knowledge of forensics are deemed experts. I am talking about how wrong this is, how somebody who has no real expertise and so trusted to defeat the presumption of innocence it is in this context that I talk about my work at the CIA. And what I say in this document is too generic to even be classified. No CIA witness even told you this information was sensitive let alone classified or national defense information. In fact, the government did not even ask a single witness from the CIA whether this information was classified.

So let's go back to Exhibit 801 and take a look at the contents of this. Introduction, transcripts, certainly not part of a battle plan. Right? Search warrant, not part of a battle plan. The complaint, not a battle plan. Ethics and logical look at the charges, tyranny, conspiracy, and

conclusion. It is not a battle plan. This is a man talking about the constitutional system and how it works -- how it works and how it hurts an innocent person if you are sitting in jail.

From here I will stage my information war: and then I clearly define what that information war is. Facebook, I will rename simply who is John Galt or who is Josh Schulte. That is not a battle plan.

And then I tell you I'm going to put this up on Wordpress. And then I put it on Wordpress. What am I talking about? What does the trial evidence show you? I am talking about my innocence. I am talking about anything other than my innocence. The Wordpress I titled the Presumption of Innocence. The website is named PresumptionofInnocence.net. Do you think anybody would want to know about my opinions about the presumption of innocence? Of course not. No one actually cares but that's what I am focused on. It has nothing to do with destroying America or having a battle plan of any sort.

This is what they have given you because they have no evidence that I stole anything from the CIA. Go back and look at my words and the notebooks. These are the words, the thoughts, the thoughts about a criminal justice system that has nothing to do with anything else.

And Mr. Betances adds nothing to this testimony. I want you to just think about Mr. Betances for two seconds.

Like me, Mr. Betances is in prison. It is the prosecutors who hold his life in their hands. They want him to testify a certain way and if he does so, he can get released from prison and a visa to live here in the U.S. So of course he tells the prosecutors that he heard a few words from me: WikiLeaks, Russia, information war. This is what they want him to say and he knows it. But, at the end of the day, Mr. Betances just wants the same thing as the rest of us. He wants to be free and enjoy the precious few years he has on this earth. He is just telling the prosecutors what he knows they want to hear so he can get back to his family and his life.

And with that, I'm on my final section. Now I want to go through the formal charges and help you sort out the facts. The indictment has nine charges, nine crimes, and as you hear from Judge Furman, there is a nice checklist, so to speak, to help you decide my fate. Each count has a number of elements, it works like an AND gate. In order to convict you need to find guilt beyond a reasonable doubt for each element. So that means as soon as you find the government failed to prove any element beyond a reasonable doubt, then you must stop there and find me not guilty. You do not even need to look at the other elements. So, as we go through the elements for each count, I am going to highlight the easiest elements that the government failed to establish so if you start with those, I think you can finish up your deliberations quickly.

Count One charges me with illegal gathering of national defense information. It has three elements but I'm going to focus on the first one, taking information. The government did not even come close to proving this element of Count One. They have not answered these very basic questions: How was it taken, what was it copied to, and when was it taken.

Now, let's not forget the first hour or so we spent going through all the reasonable doubt here. Remember, they never presented to you a copy command, they never presented to you media it was copied to, a network speed, an explanation for how I can copy something from the bathroom, the transcript files that I generated. But that's not all the reasonable doubt. Recall all of the different possibilities that the government's forensic experts fail to eliminate.

The government did nothing to assuage your concerns about other possible places or origins or suspects. Overall, the evidence is clear that I did not take any CIA backups and the jury should find me not guilty on Count One.

Count Two charges me with illegal transmission of unlawfully possessed national defense information. It has three elements, I'm going to focus on the first and the last. Because you just found that I did not take the CIA backups, I therefore could not possibly possess them and both FBI Agent Evanchec and Mr. Berger did not find a single backup or any classified or national defense information from my home.

That's it. Once you find the government failed on a single element you can move on. But in case you are not convinced, element three easily fails as well and for similar reasons.

The government did not present to you a single forensic artifact that I transmitted anything to WikiLeaks. And remember those NetFlow logs? The government asked my Internet provider Verizon for those logs, it has had them for years, logs that if I were guilty would show connections to WikiLeaks and transfers of 200 gigabytes during May of 2016. But did they show that? The government's expert didn't even testify about them. Overall, the evidence is clear that I did not transmit any CIA backups to WikiLeaks and the jury should find me not guilty on Count Two.

(Continued on next page)

MR. SCHULTE: Count Three charges me with illegal transmission of unlawfully possessed national defense information from prison. Specifically, the indictment charges me with disclosing information about internal computer networks; namely, Hickok. I'm going to focus on the second and third elements here.

Count Three is based exclusively on this email. As you can see, the purpose of this email is to highlight and argue that the FBI's initial search warrant in this case was unconstitutional. Government Exhibit 812 is a 13-page document with the search warrant attached. And if you review the full document in context, you can see the point of the email is to go through and challenge the search warrant line by line. The point is not to disseminate sensitive information.

Do you recall the stipulation by the government about the information I retained in my head after leaving the CIA?

The government recognizes that I retained NDI that would be extremely damaging to national security. You see no attempt to do so in this email, an email focused exclusively on my case and in particular the search warrant. As the trial evidence shows, there is clearly no intention, belief, or indication that these two clauses are sensitive, let alone classified or national defense information and. This is important for both elements two and three.

If the information is not NDI, then element two fails.

And as for element three, the government must prove beyond a reasonable doubt that this information was willfully communicated; that a transmission occurred willfully to do something the law forbids. But you can tell from the context alone there is no willful attempt to violate the law. If the information is not believed to be unlawful NDI and not so willfully communicated, then you must acquit.

But first let's drill down into Hickok. As you can see, this email was sent on September 24, 2018, or 18 months after WikiLeaks already published information about Hickok, EDG, and DevLAN. The government even stipulated to these facts. It is not disputed that WikiLeaks published this information on the internet. If you compare the statement that the government claims to be classified with what WikiLeaks published on the internet, you will see that I said nothing more than what was already out there. I did not endanger national security or expose national defense information.

Furthermore, all the CIA witnesses testified that DevLAN was shut down right after the leaks. If DevLAN was shut down, Hickok must've been shut down too, or at the very least, no longer worked since it required access to DevLAN. Its exposure by WikiLeaks also strongly suggests it was no longer used. So how can it relate to the national defense -- how can I expose national defense information when the CIA is not even using it anymore?

If someone publishes a book about the networks the CIA used in the 1950s, is that national defense information? Of course not, the CIA no longer uses them.

Next, the government did not put a single CIA expert -- the government did not put on a single CIA expert classifier. Not one. There's no evidence in the record that this information is even classified. And while classified information is not necessarily national defense information, documents marked unclassified cannot possibly be national defense information. In fact, the evidence in the record shows that the CIA provided me the Hickok user's guide when I worked there, which they labeled as unclassified. The CIA cannot tell its employees something is unclassified and then charge them with a crime for talking about it. That's absurd. And the government showed you absolutely no evidence that Hickok was ever labeled classified or otherwise communicated to me as something that was classified. So how could I possibly believe it to be so?

So, there's a trifecta here proving my innocence of this crime. Hickok is very clearly not closely held by the government and does not pertain to the national defense and, therefore, is not national defense information.

The government's also trying to claim that my statement that 200 COG employees was national defense information. I leave this up to you and Judge Furman as to

whether or not you can even consider this, since the indictment clearly limits Count Three to information about CIA internal computer networks, not the number of personnel. Regardless, my statement about 200 COG employees is not national defense information. As an initial matter, the trial evidence makes clear that I did not have any need to know how many people worked in COG. The trial evidence makes clear that I would not have any idea how many people actually worked in COG. The government has not identified for the jury that the size of COG was 200 people, which they must in order to prove the information is NDI.

If I say the U.S. government keeps aliens locked up at Area 51, the government cannot arrest me and charge me with disseminating NDI, since this is false, to my knowledge. The government cannot closely hold false information, and false information is not related to the national defense.

The government also failed to establish that I was ever briefed on the number of people in COG or that I was told this information was classified. In fact, as noted with respect to Hickok, the government did not present a single expert classifier to testify that this information was ever classified. The failure of any of these things requires acquittal.

And it's clear from the record where the number 200 comes from. The unclassified search warrant claimed that there

were 200 employees in EDG. It is, therefore, a logical, reasonable inference that COG, another group in CCI, contained the same number of employees as EDG. Regardless, if you look at the context of GX812, the point of this was to stress that there was an entire group that had been left out of the search warrant, twice as many possible suspects.

Next, because the trial evidence clearly shows I had no reason to suspect, let alone believe, that this statement in the email was NDI, there can be no willful transmission; the jury should find me not guilty on Count Three.

Count Four is the attempt charge from MCC.

This count has the same three elements as Count Three, substituting element three's transmission element with an attempted transmission. Specifically, the government claims that I attempted to disseminate national defense information by writing information in my private notebooks that I labeled attorney-client privilege and never released publicly.

I'm going to focus on the second and third elements, and Count Four is based exclusively on GX801 and GX809. So let's start with Government Exhibit 801.

First of all, is this NDI? Check your trial transcripts. The government does not even ask a single CIA witness whether this information is classified: Not Mr. Weber; not Mr. Leonis; not Mr. Stedman; not Mr. Roche -- no one from the CIA. This information is clearly written very generically.

What basis exists to believe this information is even classified, let alone NDI?

None. The government has not even tried to prove this beyond a reasonable doubt.

And what about the attempt? Was there ever an attempt to disclose Malware of the Mind.

Defense witness Hannah Sotnick testified about this document. She told you it was given to her in April or May -- in April of 2018, and she gave it to my attorney. The trial evidence shows it was never publicly disclosed. Agent Schlessinger testified to that, and there were also multiple pages in the notebooks -- there were also multiple pages in the notebooks to rewrite this document. The government cherry-picked page 84 out of 146 and claimed that this page was somehow written to harm the United States.

And how is that possible when it was never even released?

April 2018 through October 2018 and not once ever was the document disclosed. And the record is clear that there was no attempt to release it. There is no substantial step taken. I mean at the very least, the first 83 pages must be disclosed before we even get to this page, and not a single full page was ever disclosed.

Next, the government claims that the supposed tweets about Bartender is also NDI that I attempted to disclose. As

an initial matter, the information at issue here is not NDI. The tool described in the vendor report is, in fact, Bartender. It's too generic to be national defense information. Additionally --

MR. DENTON: Objection, your Honor.

THE COURT: Ladies and gentlemen, I'll give you instructions on what constitutes national defense information. As I said before, it's my instructions that govern, and to the extent that either party states anything that is inconsistent with my instructions, you are to follow my instructions.

Go ahead, Mr. Schulte.

MR. SCHULTE: Additionally, Bartender was previously exposed before WikiLeaks exposed it a second time, at which point the CIA halted all operations. Due to WikiLeaks, Bartender, like DevLAN, was shuttered long before I ever ended up writing notebooks at the MCC. But most importantly, WikiLeaks specifically exposed Bartender nearly 18 months before I wrote about it in my notebooks.

And I'd just note for the jury this is a substitution that the judge approved for the transcripts.

Mr. Weber expressed his concern with my statement about Bartender. In his opinion, the statement is classified because it points to an operator being witting to the usage of the tool.

However, Mr. Weber then concedes that the Bartender

document exposed by WikiLeaks would have made the exact same statement. So that's it. Even if the statement were found to be classified, it cannot possibly be NDI since it was released publicly all over the internet in March 2017, eight months before I wrote about it in my notebooks at the MCC.

And finally, once again, Mr. Weber is not a classification expert. The government did not call a single classification expert. So there is absolutely no credible evidence in the record to support the conclusion that these generic statements about Bartender, a tool exposed not only by WikiLeaks but also years before, was ever classified, let alone NDI.

And what about the attempted transmission?

Well, you need not even consider that, since the Bartender information is not NDI. But even so, there was clearly no attempt to disclose this information publicly.

What evidence is in the record regarding the supposed Bartender tweets?

They were never posted online, either on the Twitter account or on the Buffer account as a planned tweet. There was never a plan -- there was never any disclosure or any plan to disclose them, which brings me to my next point -- argument.

According to the government, despite no such evidence in the record, the heroic FBI swooped in and stopped me from posting these tweets or Malware of the Mind on the internet.

Right? That is the government's argument. But then, even though this information was never published on the internet, the government then publicly disclosed it here at trial so it could charge me with a crime. Yet according to Mr. Weber, the CIA would never deliberately disclose sensitive national defense information.

Think about it. If I wrote about something that could actually endanger national security operations or something like that, would the CIA deliberately --

MR. DENTON: Objection, your Honor.

THE COURT: Ladies and gentlemen, the government is not on trial here, and its decisions about what to charge Mr. Schulte with and what it had to disclose or reveal publicly in order to charge him with that are not on trial or your concern either. Your concern is solely whether the government has proved beyond a reasonable doubt the crimes with which Mr. Schulte is charged.

Mr. Schulte, you may proceed.

MR. SCHULTE: Indeed, the fact that the government did not call a single classification expert lends substantial weight behind this argument. The information in Count Four was simply not NDI.

THE COURT: And let me say one additional thing.

The question that you'll be asked to decide is whether the information qualifies as national defense information at

the time, not today at trial. It's not today that is relevant for your consideration.

Go ahead.

MR. SCHULTE: Accordingly, the jury should find me not guilty of Count Four.

Count Five charges me with unauthorized access to a computer to obtain classified information, particularly the CIA backups. Count Five is essentially a combination of Counts One and Two and has similar elements. Count Five has a total of four elements, none of which the government proved beyond a reasonable doubt.

The government did not prove beyond a reasonable doubt that I ever accessed the Confluence VM. There were no forensic artifacts of a log-in to the Confluence VM or any command sent. The snapshot and reversion of the Confluence VM does not constitute access. These are authorized commands of an ESXi system administrator. These are the equivalent of performing physical maintenance to the outside of the machine -- power on, power off, etc.

Next, because I did not obtain or copy the CIA backups, the government failed to prove beyond a reasonable doubt that I ever obtained protected information. The reasonable doubt for this element is the same as I discussed in Count One, and for the same reasons I'm not guilty on Count One. I'm also not guilty for Count Five.

And finally, the government failed to prove beyond a reasonable doubt that I ever transmitted any CIA backups. The reasonable doubt for this element is the same as that discussed in Count Two, and for the same reasons I'm not guilty in Count Two, I am also not guilty for Count Five.

Count Six charges me with unauthorized access of a computer to obtain information from a department or agency of the United States. It's essentially charging me with the same thing as Count Five. It only has three elements, each of which is also contained or similar to those in Count Five, which the government failed to prove beyond a reasonable doubt for the same reasons, and we won't go into that analysis here. The jury should find me not guilty on Count Six.

Count Seven charges me with causing transmission of a harmful computer program, information, code or command by executing a snapshot-reversion on the Confluence virtual machine. It has four elements, none of which the government proved beyond a reasonable doubt.

The government has and will continue to try to argue that I lied to my management about not deleting my key to the ESXi server. However, the email I sent about revoking my keys was only for the Atlassian servers. It clearly has nothing to do with the ESXi server or other system administration, and this is the interpretation of both Mr. Leonis and Mr. Weber. It clearly has nothing to do with the ESXi server or other

system administration.

Furthermore, I later send an email to Leonis, informing him about my accesses to the ESXi server. So even if the previous email was vague about what accesses I retained, this email was crystal clear. I tell Leonis about my accesses and request their transfer. Leonis does not ask me why I still have server access. He does not say I thought you destroyed your key to that server. He says nothing like that. In fact, I don't think it's in evidence that he ever responds.

Furthermore, I continued to administer the ESXi server until I resigned. My access key even remained on the ESXi server after I resigned -- from November 2016 until the FBI seized it in March of 2017. And according to Mr. Weber's testimony, he was not a Linux administrator. So who was left to administer the server?

And the reason the government will try so hard to convince you I lied or hid back-door, secret accesses to the ESXi server is because that root server key authorized me to do anything. The trial evidence clearly shows that as a primary system administrator with the sole root access key and the individual who literally owned the server, according to CIA accountable property, I had both the ability and authority to execute any command. The CMI property holder is like the title to a house, and the root server key is the keys to the front door. For all intents and purposes, I was the owner and

accountable property holder. There was no hacking, stealing, or subversion, I literally logged in to the computer with my key. Regardless, performing system snapshots and reversions are not harmful computer commands. This is not a virus or malware. It's literally routine maintenance. This is like saying getting a routine oil change constitutes theft. It just makes no sense.

Next, the government did not even remotely show any intent to damage or deny a service to a computer. These are normal ESXi commands. Each step of the process is required. The initial snapshot on April 20, 2016, was required to preserve the state, to save all the data on that server between April 16 and April 20, 2016.

Next, the trial evidence shows the reversion was typical system administration and maintenance. Reverting the system to April 16, 2016, did not cause any damage because the April 20, 2016, snapshot saved the data.

Next, the reversion back to April 20, 2016, was absolutely required. The government makes it sound as if the purpose of this final reversion was to erase all records on the computer during that time. That's simply not true.

Think about it. What was going to happen to all the data that was created or modified in Confluence between April 16 and April 20, 2016?

If I left the system on April 16, that data would be

irrevocably lost. It was absolutely critical to execute a final reversion to restore this data. Failing to do so would constitute harm to the system by losing this data.

Finally, the reversion could not have possibly caused any damage to Confluence VM itself, since there was no log-in or access of the Confluence VM during the reversion period. So ultimately, there was no damage to the Confluence VM. It was left in the exact same state, when it all started, that April 20, 2016, snapshot. A reversion is essentially like losing changes in a file that you close without saving. That's what happened here. So if there are no changes to that file -- *i.e.*, no log-ins or access to the Confluence VM -- then there is nothing wrong with closing the file without saving it*; i.e.* reverting. And as previously noted, this final reversion was necessary to preserve the modified data between April 16 and April 20, 2016.

Simply put, the government did not establish there was any damage to the Confluence VM caused by the reversion.

Finally, the government does not even present any evidence to support final element: harmful consequences.

What were the harmful consequences of the snapshot-reversion? Did it disrupt the commuter system used by national defense? How could it when the system resumed normally from the April 20, 2016, snapshot?

There's no email in the record of anyone raising any

alarms about this. The government simply did not even attempt to prove element four. The jury should find me not guilty on Count Seven.

Count Eight also charges me with causing transmission of a harmful computer program, information, code, or command, but this time for deleting log files on the ESXi server. And likewise, the government failed to prove all four elements beyond a reasonable doubt.

As we've already seen, the root server key allowed me to perform any function on the ESXi server.

Next, there is no evidence in the record at all that there was any intent to damage the ESXi server. Additionally, there's absolutely no evidence that deleting the log files caused any damage to the system. There is no evidence that the log files contained viable data and were not corrupted, and there's nothing the log files would have recorded that wasn't already recorded through the transcript files found on my CIA workstation.

Finally, like Count Seven, the government did not even attempt to establish any harmful consequences from the log deletions. To the extent the government attempts to argue the loss of the log files, it is not clear from the record that those particular log files from April of 2016 would exist in March of 2017. Mr. Weber testified on direct that he typically deleted old log files. So even if the April 20, 2016, logs had

not been deleted, would the system administrators have deleted those files in October of 2016, December of 2016, February of 2017?

The log deletion policy is not in the record, and the government failed to establish that there were any harmful consequences from the deletion of these files in April of 2016. The jury should find me not guilty on Count Eight.

Finally, Count Nine charges me with obstruction of justice. It has three elements, and the government proved none of them beyond a reasonable doubt.

With respect to element one, the government established that Agent Evanchec issued me a subpoena at the conclusion of our first conversation outside the Pershing Square diner to appear before a grand jury on March 17, 2017. But that's it. The government did not establish the scope of this procedure or that it continued to exist into June of 2017.

With respect to element two, again, the government only established my knowledge of the proceeding after the meeting at the Pershing Square diner ended and did not establish that I knew this proceeding would or could extend into June of 2017.

As to the third element, the government did not prove that four of these statements were false, and the remaining three implicate the OIG email that was later reclassified after my initial classification of unclassified. But the government

first failed to show how these statements about the OIG email, which could not have even been communicated to the grand jury, since they were quickly shown to be incorrect when the OIG email was discovered in my apartment, hours later, were ever delivered to the grand jury or how they could possibly obstruct or impede the grand jury investigation.

The government also failed to show that these statements were deliberately false as opposed to mistakenly incorrect, particularly because the trial evidence shows that Agent Evanchec did not identify the OIG email as the email I labeled as unclassified, never presented me a copy or permitted me to conduct a review at my apartment.

Finally, the record evidence is very clear that the OIG statements were made before I was issued the grand jury subpoena and, therefore, before I had any knowledge of the proceeding. The jury should find me not guilty on Count Nine.

Just go back, when Judge Furman is instructing you on the jury charges, to the facts as they have come out, and you will see that the government has failed to prove guilt beyond a reasonable doubt.

Look, I'm going to sit down now. My work is almost done. It's been three weeks of trial and a lot of evidence, and my work is almost done and your work is just about to begin. So as you undertake this work, I ask you to ask yourself about these witnesses. Do I trust these witnesses?

Do I trust these people? Do I trust the information they gave me? If I were your relative or your friend, is this the kind of proof that would be enough? Would you trust the evidence?

When you go back to deliberate, I ask you to please think of all the gaps that the government is asking you to fill. Ask yourself why are there so many gaps that they want me to say it has to be this and it has to be that. It's not your job to fill these gaps. It's not your job to take the assumptions that the government has given you. They are not evidence. Do not do what they are asking you to do. Do not fill those gaps.

Your job as jurors is to put the government to the task of proving guilt beyond all reasonable doubt, and that is all I ask you to do. After this, I won't be able to speak to you again. This is my one shot of telling you about all the evidence that proves that I'm not guilty. The government gets to give a rebuttal. The government gets one final chance to stand up and answer everything that I have just said, and I won't be able to answer back. I just won't have the opportunity. But you will.

You know everything that I know, and no matter what Mr. Denton says next, you will be able to answer that. All you have to do is say what would Mr. Schulte say in response to this argument, and you will have the answer. Because in three weeks, you know all of it. So I ask you, no matter what

Mr. Denton says, ask yourself the four questions I asked you at the beginning.

As I told you during my opening, all I ask from you is to grant me the presumption of innocence. I ask that you realize how my life is in your hands. I ask that you put yourselves in my shoes and treat me as you would like to be treated if you were here and I were there. If you do this and go into the deliberations with an open mind, I am convinced you will reach the only possible verdict -- that the government failed to prove beyond a reasonable doubt that I am guilty of any crime because I am, in fact, innocent.

Then, hopefully, justice will be done and we can all go home.

Thank you.

THE COURT: Thank you, Mr. Schulte.

All right. Ladies and gentlemen, first of all, this is probably so obvious that it doesn't need to be said, but I'll say it anyway. Mr. Schulte's slide deck had a couple clips from, I think, commercially released movies. If I'm not mistaken, one was Mission Impossible with Tom Cruise. Suffice it to say those are not evidence. Those are movies. He just used them for demonstrative and argumentative purposes, and that's fine. I just want to make clear that they are not evidence and obviously don't reflect what happened or didn't happen in this particular case.

All right. You've been paying careful attention, I've seen, for quite a while now. I know we've pushed through the lunch hour. I hope you guys had something to eat in the earlier break. So we will take a break now just so you can stretch, eat some more, if you like, use the restroom, etc. Let's take another half-hour break after which the government will have an opportunity to give its rebuttal. I will see where we are at that point. I think odds are pretty high that we won't get to the instructions today, because I don't want to begin them and then break in the middle for the day. So we'll see, again, where we are, but we may have to do that tomorrow morning.

In any event, keep an open mind. Don't discuss the case. Don't do any research about the case, and enjoy your break. It's 2:02 now, so please be ready at 2:30, and we'll start as promptly thereafter as we can.

Thank you.

(Jury not present)

THE COURT: You may be seated.

All right. Mr. Schulte, that was very impressive, impressively done.

MR. SCHULTE: Thank you.

THE COURT: Depending on what happens here, you may have a future as a defense lawyer. Who knows?

Anything to discuss?

MR. DENTON: No, your Honor.

THE COURT: Mr. Schulte, anything for you to discuss?

MR. SCHULTE: No.

THE COURT: All right. I'll see you, and please be back at 2:30.

Thank you.

(Recess)

THE COURT: Mr. Denton, are you ready to proceed when the jury gets here?

MR. DENTON: Yes, your Honor.

THE COURT: While we are waiting, I will give you a heads up, I understand the jury is about to be here. If you haven't already, just for our records, if each side could give their slide deck from their closings so that we have them I think it would be helpful and a good idea but no rush.

The jury should be here in just a minute.

THE DEPUTY CLERK: Jury entering.

(Continued on next page)

(Jury present)

THE COURT: You may be seated.

Welcome back, ladies and gentlemen. I hope you enjoyed your break. We will continue, as I told you earlier, with the government's rebuttal. I would ask that you give Mr. Denton the same careful attention you have given the previous two summations. I also just remind you, again, that what the lawyers say, what Mr. Denton says, it is not evidence.

With that, Mr. Denton, you may proceed.

MR. DENTON: Thank you, your Honor.

MR. DENTON: Well, ladies and gentlemen, I get the last word here. As you heard this morning, the government has the burden of proof in this case and that is extremely important, that is what ensures that Mr. Schulte is getting a fair trial here. Because the government has the burden, we get one last opportunity to present this case to you and I want to talk a little bit about that burden because it is something that we embrace, like Mr. Lockard said, it is the burden to prove his guilt beyond a reasonable doubt. And Mr. Schulte talked a lot about reasonable doubt. And Judge Furman is going to give you some very specific instructions about it but I really want you to think for a moment about what it is and the words basically defines themselves. It is doubt based on reason. It is not speculation, it is not suspicion, it is not a guess, or a whim. And most importantly, like everything in

this case, your decision about whether the government has proven Mr. Schulte's guilt beyond a reasonable doubt must be based on evidence, based on the exhibits and the testimony that you heard in this case.

There are a lot of things that I think you just heard from Mr. Schulte that sounded probably very familiar to things that he tried to get witnesses to say when he was cross-examining them; his questions, trying to get those things out. His statements now about things that he presented to you as facts are not evidence. When the witnesses said no to him, that's the evidence.

MR. SCHULTE: Objection.

THE COURT: Objection is overruled.

Again, the lawyers argument is just argument. It is your recollection of the evidence that controls.

MR. DENTON: So, ladies and gentlemen, as everybody told you at the start of this case, the single most important thing we can ask you to do is pay close attention to the evidence and base your decision on that, so I want to talk about some of the things that Mr. Schulte talked about that do have answers in the evidence.

Ms. Cooper, if we could put up Government Exhibit 1703-1, page 44?

While we are working on that let me explain what I want to talk about here. That page is the timeline that

Mr. Leedom put together that shows the reversion of the Confluence virtual machine on April 20th and the deletion of the log files that happened. Mr. Schulte does not dispute that he did those things. He said, well, that was just normal systems administrator activity. That's not what the evidence showed.

MR. SCHULTE: Objection.

THE COURT: Overruled.

MR. DENTON: Mr. Leedom specifically told you nothing about that was normal. Nothing about that was consistent with normal systems administrator activity. That was consistent with somebody covering their tracks. That's what the evidence shows but I want to talk through what exactly it shows because your common sense will tell you that, too.

The reversion that the defendant did on April 20th, from the snapshot he took that day from the snapshot that they made on April 16th essentially did one thing, it gave him back administrator access to the Confluence virtual server. That's the change that happened on April 16th. That's what he is going back to, that's what he is re-enabling by doing that reversion, he is putting his access back into the live machine. He is letting himself be an administrator again. 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.

Being an administrator on the Confluence vertical server on April 20th mattered to Mr. Schulte because that's what he knew he needed to get to that backup folder. He had found out just days before that he couldn't get to the Altabackups without being an administrator and so that's what he did. And there is a piece that doesn't make any sense about his reversion either. You heard about the use of snapshots, you heard why they have some place in normal function. There is a real legitimate purpose for it. It's to be able to undo things that went wrong. If there is a problem at 5:29 p.m., you can roll it back to something before then and that makes the problem go away. What doesn't make sense is going back to the snapshot with the problem at the end of the time, going back to bkup. The snapshot that he created is the piece that

makes no sense here because that would have undone whatever he tried to do as normal maintenance. No evidence, not even an offer from him what that maintenance was. But if he had been doing something to try to fix the system the reversion would make that all go away. The only purpose of the re-reversion back to bkup at 6:51 is to hide everything that happened in between. And that's what the evidence showed. That's what the witnesses who testified explained to you. That's the effect of that action. It erases what happened during that hour and a half of time. And you know what happened in that hour and a half of time.

Ms. Cooper could we put up 1203-27, please?

That's the time when those March 3rd files in the Altabackups are accessed, right in the middle of that reversion; 5:42 and 5:43. 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.

And you know that the reason the defendant stole it is because he was angry. He has tried to tell you that, no, he just made lemonade out of his life. And Judge Furman is going to give you some instructions on motive and intent and knowledge and one of the things you will hear is that it is not possible to look in someone's mind. Your decision on that has to be based in the evidence that surrounds people's actions, the things they've done, the things they've said, and frankly, ladies and gentlemen, I don't think the idea that Mr. Schulte was calm and collected and moved on with his life is supported by a single piece of evidence.

Even the little things, like having his access taken away to part of Brutal Kangaroo, he is literally still writing about years later. He is complaining about what happened when Jeremy and Karen wronged him and set him up in 2018 when he is in prison. That's not a man who lets go, that's a man who holds a grudge. And a man who holds a grudge is one who is prepared to, as he put it himself, do whatever it takes. Because he thinks that the normal rules don't apply to him.

Going back to April 20th, his explanation for deleting all those log files was that SSH key meant I was allowed to do

whatever I wanted. That's what he said to you today. It's the same thing that he said to Sean Roche when he told him I could get my access back any time I wanted. It is the same thing he told CIA security when he said access controls don't apply to me. But you heard from almost every single witness in this case, and honestly your common sense as people who live in the world and have to interact with others tells you, there is a big difference between being able to do something, between having the power, and having permission; having authority, having authorization to do something. Those are not the same things. And you heard about that in particular in the context of this network at the CIA, that it was a network that relied on trust, that it relied on empowering people to make things work for others, to serve as administrators, to protect the system. And that was the trust that he violated.

And, by the way, when we talk about deleting those log files on April 20th, he again tries to tell you, well, this was some routine thing, look, this is only 20 minutes apart. No evidence whatsoever of that in the record. No evidence that this was normal. And in fact, the evidence shows quite the contrary. He is not repeating a cycle every 20 minutes, he is searching for new log files and deleting more. And is not just deleting any log files, he is deleting the newest log files, which every witness told you is something you would never do, you would always want the newest log files. So why is he

deleting the newest log files? He is hiding what he did, he is hiding what he did in that time.

Those are important things for you all to recognize because, as he pointed out, Count Seven and Eight in this case concern specifically that reversion and the deletion of those log files. There is no question he did those things. Once you reach that conclusion on those counts, the question that you then have to ask yourselves is why? What was the point? What was all of that hiding? And he comes up with, you know, some theory that, well, it could have been a different backup file, it could have been a touch command, I was too smart to steal it this way, I would have stolen it much better. But that's not what the evidence shows. The evidence shows that that backup file was stolen at that time. That's the evidence. Everything else is speculation.

He makes a lot of the fact that there is no copy command and Mr. Lockard talked about this already so I'm not going to belabor the point but I think it is important in this context to recognize how he is trying to confuse you about where evidence would be. He tried to put up a whole bunch of, you know, essentially faked log files to say, well, this is where the command would be, this is where it would be. He is actually totally wrong about that. The logs that he was showing you are logs from that actual server, not from the Confluence virtual machine, not from the actual computer that

has the connection to the Altabackups, not from the place that the experts told you is where the copy command would be and that it was erased by the reversion. And you know that also again from your common sense.

There is no question that backup file was copied. It's on WikiLeaks. Right? It was copied at some point by somebody. All of the other evidence shows that it was Joshua Schulte but there is no question that it was copied. So where is the copy command? Where was the time when the evidence of that would have been deleted? Where is it that caused that command to go missing? It is in his actions. It is in what he did on April 20th when he reverted that system in a way that makes no sense except if you are covering up a crime.

Now, there are a number of other things that he talked about about his actions on April 20th, and I think a lot of them, again, you will find there is no support for in the evidence. He tried to suggest that he couldn't have stolen these because he was going to the bathroom. First time we are hearing that. Also, if you look at the map that he showed you, the door is like steps from his desk, it's not as if he couldn't get to his desk and do these things. Nor is it like he has got to sit there. He asked you to think about any number of things you would do. How many times do you download or copy something and walk away from your computer for a minute, get a coke and a smile, and then come back? That tells

you nothing. But the question is, where is the evidence -- and it's not there.

He also said a number of things about what wasn't there with respect to the transmission to WikiLeaks. And, ladies and gentlemen, as Mr. Lockard said, first of all, this is at a certain level a pretty easy question, it's on WikiLeaks, they got it, it was transmitted, Mr. Berger explained that. 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.

And, by the way, with respect to what he did at home, he again tries to put words in the mouths of witnesses and say, well, this is all entirely consistent with this other thing I claimed I was doing. But, actually, remember when he tried to push that with Mr. Berger, kept trying to get him to say, oh yeah, this is the program you would use if you were setting this thing up. Mr. Berger kept saying no, it is actually not, this is not what I would use that for, this is something you would use to really nuke your computer, this is not what you

would use for that purpose.

And he tries to get you to focus on little things in isolation. It is kind of funny he had his own circle and a line thing because what he did was talk these little pieces and not look at the fact that what essentially he is doing is going down the WikiLeaks checklist.

Remember, Mr. Berger put up those screenshots from the WikiLeaks onion page, that dark web page that you access through TOR. First of all, you need TOR to get there. He downloaded a new version of it on April 18th. They tell you to use Tails as an operating system that allows you to hide all of your activity. He gets that on April 24th. It tells you to figure out ways to delete data, especially if you are at high risk. Awfully coincidental that all of a sudden after having stolen that data, for the first time in ages he is researching how to kill data, how to erase hard drives. And then it says at the end of that list, that checklist from WikiLeaks, if all else fails, basically, dump the whole computer. And he did the digital version of that. He didn't throw it in the river but he completely wiped it. Total fresh start in early May.

And so, ladies and gentlemen, Mr. Lockard and I have never shied away from being candid with you about the effects of the defendant's conduct on the evidence that is available, the things he deleted that mean there are things we can't show. But what it does show is that the defense that he just put on

for you is a defense that has been years in the making, setting up these lines like there is no copy command --

MR. SCHULTE: Objection.

THE COURT: Overruled.

MR. DENTON: -- that you don't have the evidence of transmission from my home computer. Those are all things that he was preparing by taking these actions through the spring of 2020.

Now, ladies and gentlemen, I want to skip ahead for a moment because I really don't want to keep you too long here and talk about the defendant's conduct in 2018. First of all, he could not be more wrong that the purpose of these charges is to somehow insult him or otherwise cause you to view him in a negative light. Judge Furman has instructed you many times that where these crimes happened, the fact that he was incarcerated at the time, is only relevant to where it happened and not anything that you should consider against him, you should not view him as likely to commit a crime or anything because of that. And, as he said himself, these are serious crimes and I can say that they would be just as serious if they were committed from a penthouse on Park Avenue. The fundamental point is to focus on what he did. And not just on what he did in the context of the crimes but what he said, what he actually wrote in some of these things.

Ms. Cooper, is there any chance we can do Government

Exhibit 809 and go to page 5, please?

This is the defendant's to-do list. Look at what he circled. Delete suspicious e-mails from my gmail. Literally written down: Delete suspicious e-mails. Going down he is talking about erasing the phone, about resetting the IMEI, about all of these ways that he can hide activity. This isn't a guy who is interested in bringing the flaws of the criminal justice system to light, this is someone who is hiding, who is hiding the things that he has done wrong.

Ms. Cooper, can we then go to page 10 of this exhibit?

I'm going to talk about the top corner of this that we have talked a bit about quite a bit that describes Bartender but I want you to just focus for a second on the rest of this document for a moment. He is impersonating someone. He is claiming that I'm a former co-worker of Joshua Schulte and I know he is innocent, I know exactly what happened. Everything he has been telling you is nobody knows what happened but all of a sudden here he is, Joshua Schulte, pretending to be someone else and saying he knows exactly what happened? It's a lie. It's false. It's designed to try and portray him as innocent and one of the things I think you are going to hear from Judge Furman, when he gives you his instructions, is that it is reasonable for you to infer that an innocent person would not find it necessary to invent an explanation that would establish their innocence. And that stands to reason, that is

just your common sense. Someone who is actually innocent of a crime is not going to pretend to be someone else so they can put out stuff ranting about Donald Trump and the FBI as a way to claim their innocence.

But let me focus for a moment on the actual national defense information here because I think the defendant has really tried to obscure this. He spent a lot of time talking about his articles. He left up on the page his whole redress of grievances. Nothing about the MCC charges is directed at any criticism the defendant has of the criminal justice system. That is not what is at issue, that is not what he is being prosecuted for. And Judge Furman is actually going to give you very specific instructions about the exact parts of his writings that are at issue in those counts.

So this one is a good example. If we look at the section at the top, he talked a lot about how, well, Bartender was in WikiLeaks, bartender was already in WikiLeaks so, you know, that's -- it can't have possibly been damaging for me to reveal this. But that's not the detail that matters. You heard from both Jeremy Weber and Frank Stedman that no one has ever associated Bartender with that tool in a vendor report. And you heard from them why that is actually very significant and puts people at risk because what WikiLeaks released, the information about how Bartender works and what it does, tells people what the capability of the CIA is. That's bad enough.

But associating it to the vendor report, which I think they talked about being, when tools are caught in the wild, would allow an enemy to figure out when and where the CIA had run an operation with that tool. And as he himself says, it is a tool for operators to use for people, for those who have made common cause with the United States and are willing to help us collect intelligence overseas. And what he was prepared to do to authenticate himself as a fake co-worker of himself is to out the times when human beings conducted operations for the CIA. And you heard from every witness who was asked about that, what a big deal that is and that's not in WikiLeaks.

Ms. Cooper, if we could go to Government Exhibit 812 and go to page 3? And if we can blow up the second paragraph, please?

Here, too, Mr. Schulte tries to focus on Hickok was out there, Hickok was out there. That fact was there. But that's not really what matters here. You heard from Sean Roche why details about the number of people that the CIA assigns to groups might, to a casual observer not necessarily seem like the biggest deal in the world but to them it is because other countries have their own CCI, other countries have their own intelligence apparatus that will take pieces of information like this and, as he explained to you, be able to figure out things like where those people might be based, how many resources the CIA is devoting to a particular type of mission

and particular work. And that's the kind of thing that really can provide an advantage to an enemy. It might seem like a small detail but sending it to the Washington Post is not.

And on this point, Mr. Schulte made a whole big deal about how he didn't intend to hurt anybody with this, he just intended to express his criticism of the search warrants in this case. These espionage counts are complicated, I'm not going to lie to you. And Judge Furman is going to give you some pretty detailed instructions about what the government has to prove. Frankly, I think you will find that other than the top line of what each element is there is not much agreement between what Mr. Schulte said and what the Court's instructions are so you should follow the Court's instructions. But, one of the things that you will hear is that there is no element of that offense that requires you to believe that Mr. Schulte intended to harm the United States. The requirement is that it be national defense information and that he willfully sent it to someone who couldn't receive it -- a Washington Post reporter.

Ladies and gentlemen, I'm reaching the end here and I want to sort of close where I started, which is with the evidence. There is a line I have always been fond of from John Adams that facts are stubborn things and whatever our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of the facts and the evidence. Mr. Schulte's

wishes do not alter the evidence. You have heard the evidence for three weeks. You have seen the witnesses. Your observations are evidence as well. It is time for you now do what all of us asked you at the beginning which is reach a verdict that is based on the evidence. Those stubborn facts, that whatever gloss Mr. Schulte tries to put on them, can't hide what he did on April 20th, 2016 and why he did it. He is the one who broke into that system to get back administrator access he knew had been taken away from him. He is the one who knew that that was the access he needed to get to those backup files. He is the one who took that backup, the backup that he sent to WikiLeaks that you know is there, that you know forensically is the same file because of that error that he never even mentioned. Those stubborn facts prove that that is what Mr. Schulte did. They are what proved that he is guilty of the crimes charged in this case.

Thank you.

THE COURT: Thank you very much, Mr. Denton.

Ladies and gentlemen, it is 3:06 which puts me in a bind because that's enough time to get most of the instructions done but it might mean that we would push past 4:00 if I started them. I did tell you that we would end at 4:00 so I don't know if you have organized your lives based on that, in which case I think the better course would probably be just to do them tomorrow. And, it has also been a long day and it is

an important part of the process that you listen to the instructions and you pay careful attention to them so I guess I am looking for a little bit of a sign from you. If folks would prefer to call it a day there -- I am seeing a bunch of nods so that's a signal. So, I will call it a day there and we will start fresh with the instructions tomorrow which is the final step before you begin your deliberations.

So, let me underscore the instructions you have heard many times. Do not discuss the case. Sorry, you have now heard all of the evidence, seen all the evidence and heard both sides' argument. You have not heard my instructions, that is quite important, nor have you begun your deliberations. You will have plenty of time to talk about it once you begin your deliberations so for now, as tempting as it may be, do not discuss the case.

In addition, I am sure your minds are working and you are thinking about the arguments that each side has made and conclusions you should draw from the evidence but you should also continue to keep an open mind.

Deliberation is a very important part of this process. You will have an opportunity to hear from your fellow jurors and that may influence things and it is critical you continue to keep an open mind. So don't discuss the case, continue to keep an open mind, don't do any research about the case, don't read anything about the case or anything of that sort.

Please be back in the jury room same time tomorrow. In addition to the normal breakfast that you will hopefully find there, we will be -- you will find some lunch order forms. That's because once your deliberations start you basically are confined to the jury room for the duration of your deliberations and to enable you to have lunch while you are there. Obviously, that's the point. So there will be some lunch order forms, each of you can fill them out, and then before the day begins Ms. Smallman will collect them from you and during your deliberations lunch will be delivered directly to you. We are a full-service operation here.

Other than that, we will start with the instructions tomorrow. I would estimate they'll take an hour to an hour and a half and your deliberations will begin and, as I said before, we will end tomorrow at 3:00 -- either when you return a verdict or 3:00 whichever is earlier but I will give you further instructions about that tomorrow.

So with that, admonitions and instructions in mind, I wish you a pleasant afternoon and evening. You are excused and we will see you tomorrow morning.

(Continued on next page)

(Jury not present)

THE COURT: You may be seated.

The case was well argued by both sides, well tried by both sides. A couple housekeeping matter before we break for the day and if you have anything to raise I will hear that as well.

First, I think that we now have what at least the government thinks is all the evidence in the record so for what I understand is two exhibits, one is Defendant's Exhibit 410-A, that is the redacted version of the Wordpress returns if I am not mistaken, and Defendant's Exhibit 809-1, which is the better quality color copy of one of the notebooks. That one we do have a copy of it but the copy we have still has those names and phone numbers which I think were going to be redacted. So, I think those are the only two exhibits that we still need and would ask you guys to make sure that we get them so that we can add them to the jury's folder.

Any problem with that? Mr. Schulte, I assume they're in your possession.

MR. SCHULTE: Yes. I just provided them to the government 15 minutes ago or so, so.

THE COURT: Great.

Second, I just want to make sure -- well, I got a copy of the indictment which I also plan to load onto the jury system. It does have Judge Crotty's initials since he was the

presiding judge when the indictment was returned. I directed my deputy to redact those but in a manner that doesn't even reveal that they were there, that is, white them out. I assumed everybody would be OK with that.

Mr. Lockard is nodding.

MR. LOCKARD: Yes, your Honor.

THE COURT: Mr. Schulte?

MR. SCHULTE: Yes.

THE COURT: Next, Mr. Schulte, have you confirmed that the exhibits that you received from the government are an accurate reflection of what is in evidence?

MR. SCHULTE: Yes. I believe so.

THE COURT: OK. Great. So once those last two exhibits are added that should be hopefully a complete set.

Two other questions, one is the transcripts of the two video recordings, 508-T and 509-2T. I don't know if they're included in what is being sent to the jury. Obviously, for the most part, they're just demonstratives and it is the recording that is evidence. On the other hand, to the extent that they contain substitutions, I told the jury that for those purposes they are the evidence and for that reason I think there is an argument for including them.

MR. LOCKARD: We did include them for exactly the reason the Court just identified because they contained the substitutions that are evidence.

THE COURT: Mr. Schulte, any objection to that? It seems appropriate.

MR. SCHULTE: I think that they should not come in unless the jury asks for them because what is actually in evidence is the video, and it is in English. So unless they specifically request for the audio, I just think the video should come in.

THE COURT: Normally I would agree, but given that I instructed them that where something is redacted or substituted it is the transcript that is evidence, I think that necessitates them going in as well. So, if they are already included, then that is what I think should happen.

And then the last on my list is the question that we, that was posed yesterday about the second classified exhibit. Again, Government Exhibit 1 is marked or is not marked, whatever form it is in, it is in, and it was admitted in that form, but the log files -- I don't have the exhibit number handy -- to the extent that those are being loaded on a different laptop or being provided on some sort of disk, Mr. Schulte raised the question about their having classification markings.

What is the government's view on this?

MR. LOCKARD: So, your Honor, I think our proposal is to include that -- so the exhibit itself is a disk and the disk already has been marked with classification markings. We

could, as an alternative, have that file that's on the disk loaded onto a separate stand-alone laptop and make that available. The laptop, because of the nature of what it can house, would itself have classification markings on it. I don't think we have a strong view about classification markings or not. We do just want to make sure that there is not an accidental spill as a result of the jury not being aware of how that material should be handled. I think that's our concern.

THE COURT: That shouldn't be a big concern because they're not going to be leave being the jury room with any of the evidence and I am happy to instruct them that if they don't return a verdict they should leave the evidence in the jury room and it will be secured overnight.

MR. LOCKARD: I think our main sort of -- this may be a hypothetical concern but if it was on an unmarked disk that could be inserted into an unclassified disk reader, that would present a problem. If that's not a risk then it is not something we would worry about.

THE COURT: Are you telling me it was entered in the form of a disk and the disk already has a classification marking?

MR. LOCKARD: That is correct.

THE COURT: So I guess, again, if it was admitted in whatever form it is admitted, it is admitted in that form. The question is just how the jury would access it, what are the

options on that front.

MR. LOCKARD: So the options are, I mean, essentially they're going to need a stand-alone and the question is should we just have it with a disk reader and the disk, as marked, or should we just load the file onto the laptop and have them access it that way.

THE COURT: Can they, when you say disk reader, would the disk reader -- in other words, can the --

MR. LOCKARD: They're going to need a laptop regardless, I think.

THE COURT: Right, but can the laptop not have a classification marking and then they can just put the disk in? Again, the disk may have a classification marking but if that is how it is admitted then it is in evidence in that form. As long as they can read it and as long as there is no issue with respect to reading it on a computer or drive that is not itself marked, that seems to me the preferable way to do this.

MR. LOCKARD: That may be possible. We will have to work with our IT and security vault to make that happen.

THE COURT: Why don't you see if you can make that happen and record back to us in the morning.

Mr. Schulte, anything you wish to say on that front?

MR. SCHULTE: Yes.

The defense's position is simply that we don't think there should be any markings on it so if we are able to figure

something out for that, I think that's a good way to go. Obviously there has to be some way for them to actually read the data so if we want to just put that on another computer instead of having the disk or somehow do something like this to make it easier, I'm open to that. I don't think it --

THE COURT: Well, let me say the following. Again, whatever is in evidence is in evidence, and if it's already marked it is already marked and should go to the jury in that form. What I agree with Mr. Schulte on is if we are giving them something else, that is to say a laptop with the information on it or laptop to read the information, I don't think we should be adding to what has been in evidence anything that -- I mean anything other than a vehicle for the jury to view it, that is to say, it shouldn't convey any information and a classification marking on that would, I think, so I think his point is well taken on that score.

I will leave it to the government to try and solve this conundrum but it seems to me if the disk is in and it is marked, then sobeit. But, if it can just be given to them with a laptop to use to read it, then I think we have no problem and that's the solution.

But why don't you consult with your people and we will circle back to this in the morning.

MR. LOCKARD: Yes, your Honor.

THE COURT: Anything else from the government?

MR. LOCKARD: Nothing else.

THE COURT: Mr. Schulte, I may as well ask my periodic question just to confirm that you continue to control your defense, that to the extent you are consulting with Ms. Shroff and Ms. Colson, as you have done throughout the case, you are doing so on your own volition and because you are seeking their advice and not unsolicited.

Is that correct?

MR. SCHULTE: That's correct.

THE COURT: Anything you would like to raise before we adjourn for the day?

MR. SCHULTE: I was wondering if there was any way we could get the final jury charge copy that the Court had put together.

THE COURT: Sure. I don't see any reason not to. We have copies here. I was prepared to proceed directly into the charge so if each side wants one copy, that's fine by me.

Anything else, Mr. Schulte?

MR. SCHULTE: No. That's it.

THE COURT: All right. Very good. So, with that, please be here by 9:00 tomorrow so we can start promptly when the jury gets here. I will give my instructions and then the jury will begin deliberations.

Have a restful evening. Thank you.

(Adjourned to July 8, 2022 at 9:00 a.m.)