

M77Wsch1

1 UNITED STATES DISTRICT COURT
2 SOUTHERN DISTRICT OF NEW YORK

3 UNITED STATES OF AMERICA,

4 v.

17 Cr. 548 (JMF)

5 JOSHUA ADAM SCHULTE,

6 Defendant.

Trial

7 -----x

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

10 Before:

11 HON. JESSE M. FURMAN,

12 District Judge
13 -and a Jury-

14 APPEARANCES

15 DAMIAN WILLIAMS

United States Attorney for the
Southern District of New York

16 BY: DAVID W. DENTON JR.

17 MICHAEL D. LOCKARD

Assistant United States Attorneys

18
19 JOSHUA A. SCHULTE, Defendant *Pro Se*

20 SABRINA P. SHROFF

21 DEBORAH A. COLSON

Standby Attorneys for Defendant

22 Also Present: Charlotte Cooper, Paralegal Specialist

M77Wsch1

1 (Trial resumed; jury not present)

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

4 A couple quick things.

5 First of all, I will tell the jury, but I completely
6 lost track of days yesterday when I said that we would go until
7 5:00 tomorrow. I'm actually going to end tomorrow at three, so
8 you know, and I will let them know as well.

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

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

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

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

24 All right. Ms. Shroff, good?

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

M77Wsch1

1 couldn't do it yesterday.

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

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

6 THE COURT: Great.

7 Is the government ready to proceed?

8 MR. LOCKARD: Yes, your Honor.

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

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

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

14 MR. LOCKARD: I would say two hours.

15 THE COURT: OK.

16 All right. Anything to raise before we proceed?
17 Government.

18 MR. LOCKARD: No, your Honor.

19 THE COURT: Mr. Schulte.

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

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

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

M77Wsch1

1 please.

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

4 (Jury present)

5 THE COURT: You may be seated.

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

9 Let me say a few different things.

10 First, one housekeeping matter.

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

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

M77Wsch1

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

6 One other housekeeping matter.

7 When I told you yesterday that you should be prepared
8 to be here until 5:00 tomorrow, I completely blanked on what
9 day of the week it was. Since we were starting on Wednesday, I
10 got a little confused. I actually can't -- we can't -- sit
11 until 5:00 tomorrow. So we will actually break tomorrow at
12 3:00 just for your planning purposes. We'll discuss your
13 schedule more later, and that brings me to the last topic,
14 which is the schedule, just so you have a sense of what today
15 and tomorrow are going to look like.

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

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

M77Wsch1

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

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

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

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

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

M77Wsch1

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

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

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

1 With that, we will begin with the government.

2 Mr. Lockard.

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

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

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

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

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

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

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

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

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

25 In November of 2016, several months after he sent the

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

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

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

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

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

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

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

1 he released and attempted to release more national defense
2 information.

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

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

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

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

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

25 Counts Seven and Eight also charge computer crimes.

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

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

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

14 Finally, the prison transmission counts.

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

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

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

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

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

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

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

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

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

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

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

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

1 only by cleared personnel with a need to know.

2 Now, why is that relevant?

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

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

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

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

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

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

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

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

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

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

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

7 Why is the role of an administrator important?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 that was stolen, ran on OSB's server. I mentioned virtual
2 servers before, and you heard about it during trial. A virtual
3 server is a computer within a computer. Right? It's virtual,
4 meaning it's not a physical computer. It's a piece of
5 software. The effect of that for your purposes is that having
6 access to the physical computer that hosts the virtual computer
7 does not give you access to the virtual computer. It's like
8 walking into a room where there's another computer sitting on
9 the desk. You can see it, you can pick it up, you can do
10 things on the outside of it, but you have to separately log in
11 to that virtual server. It's like a separate computer. And
12 that OSB server was an OSB piece of computer equipment. It was
13 managed by and it was administered by OSB. And after March 29,
14 2016, the defendant was not in OSB, and he was not an OSB
15 server administrator.

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

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

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

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

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

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

12 Why is it a big deal?

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

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

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

11 So what does that mean?

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

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

19 But what is he doing in the meantime?

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

24 What is he Google searching?

25 He's Google searching "Confluence admin view"

1 restricted pages."

2 Now, why is that relevant?

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

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

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

14 And why would he be interested in that?

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

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

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

20 (Continued on next page)

21

22

23

24

25

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

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

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

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

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

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

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

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

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

1 system for which they have been removed.

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

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

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

1 products.

2 What else does he do on the 18th? He uses that open
3 administrator session to go into the OSB server and review
4 files and delete files. What is he reviewing? He is casing
5 the joint. He is doing surveillance to figure out what is
6 there and he is deleting files to cover up the fact that on the
7 18th he was casing, he was casing the joint. And you can see
8 here, between 6:32 and 6:49 p.m., he executes a number of
9 commands called the VI command which you heard from Patrick
10 Leedom which basically pops open a screen on the computer so
11 you can see what is in the file. So he is opening up these log
12 files to see what they're recording and he is deleting them
13 when he doesn't like what they show. Right? He is figuring
14 out where are the security cameras and how can I avoid them.
15 Not only that, he goes specifically into the Confluence folder.
16 Now remember, Confluence is a virtual machine which means it is
17 a piece of software. Software runs in a folder or is saved in
18 a folder and Mr. Schulte is looking specifically at what is in
19 the Confluence folder.

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

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

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

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

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

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

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

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

1 server is going to be moved from OSB server to ISB network
2 space. Now why is that important? It is important because
3 Mr. Schulte still has that OSB administrative session open and
4 that is the only thing that puts him in the same place as the
5 Confluence server. Now remember, this server was only on OSB
6 as kind of a historical accident. At the time that these
7 programs were adopted and installed by the CIA, the OSB server
8 was just a place that had enough space and enough firepower to
9 run the Confluence program. It was never supposed to stay
10 there, just like the Atlassian administrator privileges were
11 never supposed to stay with the developers. But now that's
12 changing and you know why. It is changing in response to
13 Mr. Schulte. So he does not wait. He has already made his
14 plans, he has already done his reconnaissance, he already has
15 the blueprints that he needs. He has already scoped out where
16 the security cameras are and he doesn't waste a minute. That
17 night he steals the backups. And as you saw from Mr. Leedom's
18 expert presentation, between 5:30 and about 6:00 p.m.,
19 Mr. Schulte executed a series of commands that restored his
20 access to the Altabackups, copied the backup files from March
21 3rd, 2016, reversed those maneuvers, and deleted a bunch of log
22 files.

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

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

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

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

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

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

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

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

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

7 THE COURT: Overruled.

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

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

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

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

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

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

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

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

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

17 Now I am going to touch briefly on one issue. I think
18 Mr. Schulte has suggested at times through his questioning that
19 maybe somebody else was using his computer this entire time. I
20 think you know very easily that that is not the case for any
21 number of reasons. You know it, number one, because this is
22 the administrator session that Mr. Schulte opened on April
23 15th. Right? This is the session that Mr. Schulte used on
24 April 18th when he was conducting his surveillance. And, while
25 Mr. Schulte is using this session on April 20th, he is also

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

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

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

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

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

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

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

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

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

1 Nuclear Option going off.

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

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

13 So you know that the defendant copied the March 3rd,
14 2016 backups. Right? You know that those are the very same
15 backups that WikiLeaks released data from. You know that in
16 part from Mr. Leedom's testimony. Remember he testified about
17 how the backups were broken, there was an error in the program
18 that created the backups that resulted in missing data and some
19 of the data that was in the backups that was supposed to be
20 linked up was not linked. And the WikiLeaks information had
21 exactly the same errors. So we know that what they released
22 came from a backup and we know that it came from the backup the
23 defendant stole. You heard the testimony of FBI computer
24 scientist Michael Berger, who went through an extensive
25 analysis, and determined that the data in the leaks came from a

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

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

15 Between April 23rd and April 30th, Schulte tested a
16 secure file deletion program called Eraser Portable and he
17 securely deleted a folder called Brutal Kangaroo on his home
18 computer. And you heard that he queued up additional backup
19 folder files to be deleted but closed the program without
20 deleting them. But you also heard how even though he did not
21 use Eraser Portable on those files, they were securely deleted
22 because the FBI forensic review found no trace of those files
23 when his computer was seized. You heard how he downloaded
24 Darik's Boot and Nuke which is designed to nuke a hard drive.
25 And he researched various Western Digital wiping utilities.

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

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

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

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

25 But, in the meantime, the defendant is getting

1 anxious. He wants to know when is the stolen data going to
2 start to come out. And you see from his Google search history
3 before July of 2016 he had about two searches for WikiLeaks, I
4 think they were both in 2010; and then one search in July of
5 2016 about the Clinton e-mails from the Democratic National
6 Convention hack. Starting in August, he is extremely
7 interested in WikiLeaks. There are 39 WikiLeaks-related
8 searches in that four-month period or five-month period. There
9 are 115 page sites. Ask yourself, why is he suddenly so
10 interested in WikiLeaks? I think the evidence suggests the
11 answer to you, he wants to know what has happened with the
12 stolen data that he sent and when is it going to come out.

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

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

4 It was devastating.

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

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

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

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

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

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

21 Now, Mr. Schulte spoke with the FBI again, this time
22 at the U.S. Attorney's office. He was interviewed on March
23 20th and 21st, back to back interviews. And during those two
24 days Mr. Schulte was asked how the leak could have happened.
25 And what's important to you is he offers up some ways that he

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 information that only a CIA officer would know. Right?

2 Mr. Schulte knows that this information is not public. It does
3 not authenticate you as a CIA officer to talk about something
4 that you can find on Wikipedia.

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

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

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

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

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

13 (Continued on next page)

14
15
16
17
18
19
20
21
22
23
24
25

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

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

13 Count One charges illegally gathering national defense
14 information, based on having stolen the CIA backups on April
15 20, 2016.

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

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

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

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

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

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

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

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

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

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

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

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

19 Count Seven charges a harmful computer command from,
20 first, reverting the Confluence server back to April 16,
21 spending an hour and a half in a reverted state, then
22 re-reverting to April 20, eliminating all evidence of what
23 happened in that hour and a half, and then deleting the April
24 20 snapshot. I think you've heard a lot of testimony about how
25 that is harmful to the computer system. It impairs the

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

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

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

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

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

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

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

20 Finally, the two prison counts:

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

1 to receive them.

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

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

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

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

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

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

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

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

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

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

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

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

1 there was a substantial step.

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

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

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

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

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

M77Wsch3

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

8 Thank you.

9 THE COURT: Thank you, Mr. Lockard.

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

18 A quick couple quick but still important reminders.

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

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

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

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

3 With that, you are excused. Enjoy your break.

4 (Jury not present)

5 THE COURT: You may be seated.

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

8 Mr. Lockard.

9 MR. LOCKARD: No, your Honor.

10 THE COURT: Mr. Schulte.

11 MR. SCHULTE: No.

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

16 Thank you.

17 (Recess)

18 THE COURT: You may be seated.

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

21 MR. SCHULTE: Yes.

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

24 Are we ready to go?

25 MR. SCHULTE: Yeah.

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

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

5 MR. SCHULTE: OK.

6 THE COURT: Good to go?

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

10 (Jury present)

11 THE COURT: You may be seated.

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

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

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

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

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

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

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

18 What does all of this add up to?

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

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

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

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

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

24 So let's begin with the crime.

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

M77Wsch3

Summation - Mr. Schulte

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

10 The CIA joined up with the FBI, and literally, within
11 24 hours, they focused on me, the man who had left the CIA in
12 November 2016 on bad terms. The lead FBI agent admitted that
13 they had not even interviewed a single CIA witness. They had
14 not even finished seizing the DevLAN network, let alone
15 actually reviewed it. They had not conducted any investigation
16 at all, and yet I was already the target of their
17 investigation.

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

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

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

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

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

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

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

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

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

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

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

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

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

25 You can play them again during deliberation. I was

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 Now, you heard Mr. Lockard tell you that I was
21 planning to steal the backups starting as early as April 14,
22 2016. But of course, this makes no sense. As of April 14,
23 2016, trial evidence shows I still had access to the Confluence
24 virtual machine. So if I were going to steal the backups, I
25 could just copy them directly. I could literally log in to the

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

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

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

13 MR. DENTON: Objection.

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

15 THE COURT: All right.

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

22 You may proceed, Mr. Schulte.

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

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

6 What else did Mr. Lockard tell you?

7 That I stayed up late and locked up the vault in April
8 2016. But of course, the badge records show that I did this at
9 least once every month.

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

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

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

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

2 OK. Back to the events at the CIA.

3 What happens next?

4 The OSB libraries.

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

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

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

1 meeting.

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

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

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

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

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

25 Once I finished with development on Nader, I turned to

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

10 And then what happens?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Confluence backup files were accessed on April 20, 2016.

2 Instead, what does Mr. Leedom do?

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

8 Remember his forensic findings slide?

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

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

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

25 There, it shows the source controls and Gold

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

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

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

17 And instead, what does Mr. Leedom do?

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

1 below average.

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

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

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

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

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

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

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

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

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

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

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

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

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

23 (Continued on next page)

24

25

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

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

25 But, most importantly, he has the logs from my

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

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

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

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

8 After the final reversion back to April 20th, 2016, at
9 6:51:17 p.m., that cannot even access the Confluence VM
10 anymore. The copy must finish in this time frame. Yet,
11 because he has no theory as to what device the data is copied
12 to, he cannot possibly give an estimation for the amount of
13 time the copy will take. It depends upon how fast the device
14 is. It also depends upon the network speed. According to the
15 size of the backups, that's at least 200 gigabytes, about 1,000
16 episodes of Netflix. And all in an hour and 15 minutes? You
17 can do the math. Is that possible? I mean when you need to
18 download 200 gigabytes from the Internet, can you do it in 75
19 minutes?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 MR. DENTON: Objection.

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

19 You may proceed, Mr. Schulte.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 improper with writing code and bringing it into the CIA.

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

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

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

1 5th. But even for that theory he doesn't give you any
2 forensics, any forensic evidence.

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

8 Finally, it is important to talk about NetFlow logs.
9 Whenever you use your computer at home your Internet provider,
10 be it Verizon, Comcast or whoever, they record the amount of
11 data you send and receive as well as the IP address --

12 MR. DENTON: Objection.

13 THE COURT: Sustained. Sustained.

14 Please stick to the evidence, Mr. Schulte.

15 MR. SCHULTE: Mr. Leedom:

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

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

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

25 Yes.

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

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

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

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

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

15 MR. DENTON: Objection.

16 MR. SCHULTE: It is in the record.

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

22 Go ahead.

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

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

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

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

1 for the Vault 7 and 8 release by WikiLeaks.

2 Both experts testified about this to varying degrees.
3 The point is version control which existed in both Stash and
4 Confluence and keeps track of all iterations for each file.
5 Every time you modify a file, that changed the file that saved.
6 And what this means is every successive backup contains all the
7 data from all preceding backups. March 4th contains the day
8 from March 3rd, plus the new changes. So it is really trivial
9 to go through the data and select files from a particular date.
10 So while the experts tell you it has to be the March 3rd, 2016
11 backup given to WikiLeaks, this is simply not true. They are
12 not testifying as experts at this point but as FBI agents,
13 advocates for the government. No forensic expert could testify
14 as to what files WikiLeaks received, they simply have no idea.
15 The forensics can only establish one thing, what is called a
16 lower bound. This is the earliest backup that could have been
17 taken. And the reason forensics can establish this is because
18 an old backup cannot possibly have new files. A backup taken
19 on March 3, 2016, cannot contain files from March 4, 2016.
20 Those files haven't been created yet. So if you have files
21 from March 4th, then you can establish that March 4th is the
22 lower bound, it is the absolute earliest backup that could have
23 been taken.

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

1 established. If you have files from March 4th, they can come
2 from any backup on or after March 4th. So a timing analysis
3 for version controlled backups is very limited. It can
4 establish only a lower bound and in this case the lower bound
5 is March 3rd, 2016. The data released by WikiLeaks could
6 originate from each and every backup from March 3rd, 2016 to
7 March 6, 2017.

8 I also want to talk to you just for a few seconds
9 about the document that the government keeps showing you, OK;
10 1207-27, 1207-30. The document that indicates that March 3rd,
11 2016 Confluence backup was accessed on April 20th, 2016. That
12 doesn't show it copied. I don't know how many times they
13 showed it to you. I think they showed it to every witness they
14 could find. You know, we could have made this whole process
15 more fun by turning it into a drinking game when you take a
16 shot each time the government shows you 1207-27, although I
17 don't think you would be able to walk by the end of the day.

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

1 Why isn't the April 20th backup taken?

2 There is nothing in the evidence to support any claims
3 that there was any significance at all to March 3rd because I
4 never mentioned this date. There is no evidence of me
5 mentioning this date. The only people who somehow think March
6 3rd is an important date are the prosecutors because it is
7 their mission to convict me.

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

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

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

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

8 And you know from Jeremy Weber that I was an expert in
9 Linux and system administration. Whenever the individual who
10 set up the Atlassian project leaves for an overseas assignment
11 who does he go to for help? Out of all the developers at the
12 CIA he came to me. So if I am really going to be stealing the
13 data on April 20th and all I have to do is use a simple touch
14 command to change the April 20 access time back to March 3rd,
15 2016, I could have, and it would have looked just like this.
16 That's your touch command. Look at the day now. That's a
17 simple touch command, it would have looked just like this. The
18 timestamp on the right column would have matched the timestamp
19 on the left column with a simple touch command.

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

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

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

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

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

1 functioning as FBI agents and advocates for the government.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 MR. DENTON: Objection.

18 THE COURT: Sustained.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 (Continued on next page)

15
16
17
18
19
20
21
22
23
24
25

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11 Count Four is the attempt charge from MCC.

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

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

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

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

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

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

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

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

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

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

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

5 MR. DENTON: Objection, your Honor.

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

11 Go ahead, Mr. Schulte.

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

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

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

25 However, Mr. Weber then concedes that the Bartender

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

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

13 And what about the attempted transmission?

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

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

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

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

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

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

10 MR. DENTON: Objection, your Honor.

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

18 Mr. Schulte, you may proceed.

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

23 THE COURT: And let me say one additional thing.

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

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

3 Go ahead.

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

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

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

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

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

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

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

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

1 system administration.

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

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

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

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

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

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

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

22 Think about it. What was going to happen to all the
23 data that was created or modified in Confluence between April
24 16 and April 20, 2016?

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

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

4 Finally, the reversion could not have possibly caused
5 any damage to Confluence VM itself, since there was no log-in
6 or access of the Confluence VM during the reversion period. So
7 ultimately, there was no damage to the Confluence VM. It was
8 left in the exact same state, when it all started, that April
9 20, 2016, snapshot. A reversion is essentially like losing
10 changes in a file that you close without saving. That's what
11 happened here. So if there are no changes to that file --
12 *i.e.*, no log-ins or access to the Confluence VM -- then there
13 is nothing wrong with closing the file without saving it; *i.e.*
14 reverting. And as previously noted, this final reversion was
15 necessary to preserve the modified data between April 16 and
16 April 20, 2016.

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

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

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

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

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

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

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

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

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

1 not been deleted, would the system administrators have deleted
2 those files in October of 2016, December of 2016, February of
3 2017?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Thank you.

15 THE COURT: Thank you, Mr. Schulte.

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

M77Wsch5

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

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

17 Thank you.

18 (Jury not present)

19 THE COURT: You may be seated.

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

22 MR. SCHULTE: Thank you.

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

25 Anything to discuss?

M77Wsch5

1 MR. DENTON: No, your Honor.

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

3 MR. SCHULTE: No.

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

6 Thank you.

7 (Recess)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

M775SCH6

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

3 MR. DENTON: Yes, your Honor.

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

9 The jury should be here in just a minute.

10 THE DEPUTY CLERK: Jury entering.

11 (Continued on next page)

12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 (Jury present)

2 THE COURT: You may be seated.

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

9 With that, Mr. Denton, you may proceed.

10 MR. DENTON: Thank you, your Honor.

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

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

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

12 MR. SCHULTE: Objection.

13 THE COURT: Objection is overruled.

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

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

22 Ms. Cooper, if we could put up Government Exhibit
23 1703-1, page 44?

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

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

7 MR. SCHULTE: Objection.

8 THE COURT: Overruled.

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

15 The reversion that the defendant did on April 20th,
16 from the snapshot he took that day from the snapshot that they
17 made on April 16th essentially did one thing, it gave him back
18 administrator access to the Confluence virtual server. That's
19 the change that happened on April 16th. That's what he is
20 going back to, that's what he is re-enabling by doing that
21 reversion, he is putting his access back into the live machine.
22 He is letting himself be an administrator again. And he also
23 told you just a moment ago why being an administrator mattered.
24 He spent a while talking about the Altabackups saying there
25 were no user permissions, no user controls on the Altabackups,

1 anybody could get there. But then he started talking about
2 that time when he tried to get to the Altabackups and it didn't
3 work. His answer was, well, of course it didn't work, I wasn't
4 an administrator, I was using my regular user account.

5 Exactly. A regular user can't get to those
6 Altabackups, you have got to be an administrator which, by the
7 way, puts the lie to his whole claim that there were no access
8 controls whatsoever on the Altabackups. He told you there
9 were, only administrator could get there. That's access
10 control. Not every regular person could get to it, not anyone
11 could get into that folder and steal backup files.

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

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

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

13 That's the time when those March 3rd files in the
14 Altabackups are accessed, right in the middle of that
15 reversion; 5:42 and 5:43. And when we focus on those backup
16 files there is an important piece of forensic evidence that you
17 didn't hear word one about from Mr. Schulte, which is the
18 forensic analysis that Mr. Leedom did on that error in the
19 backup script, the character and coding problem that meant that
20 the database was broken, that those links between different
21 parts of it didn't match up quite right. That's why the
22 version of Confluence that's on WikiLeaks looks so strange in
23 many respects, it is directly tied to that error in the script.
24 And what does that error do? It means that you can't use a
25 different version, you can't make March 4th look like March 3rd

1 because those relationships are broken. You can't do it as a
2 different version and so it is that backup file, that March 3rd
3 backup file that you know was the one that was stolen and put
4 on WikiLeaks.

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

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

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

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

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

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

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

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

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

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

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

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

3 He also said a number of things about what wasn't
4 there with respect to the transmission to WikiLeaks. And,
5 ladies and gentlemen, as Mr. Lockard said, first of all, this
6 is at a certain level a pretty easy question, it's on
7 WikiLeaks, they got it, it was transmitted, Mr. Berger
8 explained that. In some respects the evidence of transmission
9 is the fact that someone outside of this secure building has
10 this stuff. And so once you know that he stole it, and you
11 know that because he has admitted what he did on April 20th and
12 you know there is no other explanation for it --

13 MR. SCHULTE: Objection.

14 THE COURT: Overruled.

15 MR. DENTON: -- the fact that WikiLeaks has it proves
16 that he transmitted it.

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

1 would use for that purpose.

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

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

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

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

3 MR. SCHULTE: Objection.

4 THE COURT: Overruled.

5 MR. DENTON: -- that you don't have the evidence of
6 transmission from my home computer. Those are all things that
7 he was preparing by taking these actions through the spring of
8 2020.

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

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

1 Exhibit 809 and go to page 5, please?

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

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

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

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

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

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

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

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

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

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

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

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

M775SCH6

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

17 Thank you.

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

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

M775SCH6

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

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

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

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

M775SCH6

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

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

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

21 (Continued on next page)

M775SCH6

1 (Jury not present)

2 THE COURT: You may be seated.

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

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

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

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

22 THE COURT: Great.

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

M775SCH6

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

5 Mr. Lockard is nodding.

6 MR. LOCKARD: Yes, your Honor.

7 THE COURT: Mr. Schulte?

8 MR. SCHULTE: Yes.

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

12 MR. SCHULTE: Yes. I believe so.

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

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

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

M775SCH6

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

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

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

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

22 What is the government's view on this?

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

M775SCH6

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

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

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

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

22 MR. LOCKARD: That is correct.

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

M775SCH6

1 options on that front.

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

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

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

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

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

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

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

23 MR. SCHULTE: Yes.

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

M775SCH6

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

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

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

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

24 MR. LOCKARD: Yes, your Honor.

25 THE COURT: Anything else from the government?

M775SCH6

1 MR. LOCKARD: Nothing else.

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

8 Is that correct?

9 MR. SCHULTE: That's correct.

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

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

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

18 Anything else, Mr. Schulte?

19 MR. SCHULTE: No. That's it.

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

24 Have a restful evening. Thank you.

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