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

UNITED STATES OF AMERICA,

v. S2 17 Cr. 548 (PAC)

JOSHUA ADAM SCHULTE,

Defendant. Trial

----------x

New York, N.Y.
February 13, 2020
9:00 a.m.

Before:

HON. PAUL A. CROTTY,

District Judge
-and a jury-

APPEARANCES

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
BY: MATTHEW J. LAROCHE
SIDHARDHA KAMARAJU
DAVID W. DENTON JR.
Assistant United States Attorneys

SABRINA P. SHROFF
JAMES M. BRANDEN
Attorneys for Defendant
-and-
DAVID E. PATTON
Federal Defenders of New York, Inc.
BY: EDWARD S. ZAS
Assistant Federal Defender

Also Present: Colleen Geier
Morgan Hurst, Paralegal Specialists
Achal Formando-Peiris, Paralegal
John Lee, Litigation Support
Daniel Hartenstine
Matthew Mullery, CISOs, Department of Justice

(In open court; jury not present)

THE COURT: Good morning. We're still missing some jurors, David?

THE DEPUTY CLERK: Let me doublecheck, but yes.

THE COURT: Where's Mr. Branden today?

MS. SHROFF: I'm sorry, I couldn't hear you, your Honor.

THE COURT: Where is Mr. Branden today? He was not here yesterday.

MS. SHROFF: He was not here yesterday, and he will be here shortly, your Honor.

THE COURT: All right. I read the government's letter of February 12. It came into chambers last night around 5 o'clock. Attached to it was a memorandum from the director of officer security at the CIA recommending the imposition of administrative leave on Michael. That was done on August 19.

The question I have for you, for the government, is when did the government, the U.S. attorney's office find out that Michael was on administrative leave?

MR. KAMARAJU: We knew at the time, your Honor.

THE COURT: At the time?

MR. KAMARAJU: We did.

THE COURT: Do you know who wrote the CIA memo?

MR. KAMARAJU: I don't know the individual who wrote it. We referenced the group who wrote it, but I don't know the

name of the individual who specifically drafted it.

THE COURT: Why did the government wait six months to give out the information that Michael was on administrative leave?

MR. KAMARAJU: Your Honor, I think in our view we thought the relevant information was the underlying material that showed the underlying conclusions about his credibility, and we produced those far in advance. That was our view. We produced the --

THE COURT: You made a judgment that there was already enough information for all the cross-examination that the defendant wanted to do?

MR. KAMARAJU: We did, your Honor. As we've done in other cases, we made that determination. If we erred in that, we apologize, your Honor. We made sure that -- we apologize. We did believe Ms. Shroff had, among other things, the notes that led to immediately preceding being put on administrative leave, she had contacted his lawyer.

THE COURT: With regard to the notes of your meeting with Michael, on August 16, why there was no 302 prepared?

MR. KAMARAJU: Because those were attorney notes. The FBI didn't take those notes; the prosecutors took them.

MS. SHROFF: Did the Court want to take a copy of the notes provided to us on August 16?

THE COURT: August?

MS. SHROFF: The August 16 meeting with the prosecutors.

THE COURT: I have the notes.

MS. SHROFF: I didn't know if you had them, your Honor. I'm sorry.

THE COURT: I do have the notes. They're in the 3500 material, aren't they?

MR. KAMARAJU: Yes, your Honor. We produced them to the defense.

THE COURT: I'm going to direct that the document which led to Michael's being placed on administrative leave, it is a four-page document, be produced to the defendant.

MR. KAMARAJU: Understood, your Honor. We'll give them a copy.

THE COURT: All right. Anything else?

MS. SHROFF: Will that be now or after my cross -- I'm just joking.

MR. KAMARAJU: We're getting it.

MS. SHROFF: I was just teasing you, I'm sorry.

THE COURT: Anything else to take up this morning? Is the jury here?

MR. KAMARAJU: Nothing from the government, your Honor.

THE COURT: The jury is here.

MS. SHROFF: Will you give me a break -- I haven't

seen the document. Can I look at it before the cross? I can start now, and then when I reach a point at the end --

THE COURT: How long are you going to be on cross?

MS. SHROFF: I think I have at least 30 minutes before I read this four-page memo. I don't know what the four-page memo is. But you can let me finish, and then I will leave that part at the very end. Would that help?

THE COURT: Yes. Anything to get us started.

MS. SHROFF: That's fine. We can get started, your Honor.

THE COURT: Are you going to bring Michael in? As soon as Michael comes in, bring the jury in.

(Continued on next page)

(Jury present)

THE COURT: Good morning. Please be seated. Michael, I want to remind you, you're still under oath.

THE WITNESS: Thank you.

THE COURT: Ms. Shroff.

MICHAEL,

CROSS-EXAMINATION (Continued)

BY MS. SHROFF:

Q. March 16 is when you first met with the FBI for the first time, March 16, 2017?

A. I don't remember the date.

Q. During that interview, did you tell the FBI, when they asked you about Mr. Schulte, that you had seen no -- that you had seen Mr. Schulte go through a rough time at the end of his employment with EDG?

A. I don't remember the specific words, but I remember something like that.

Q. I'm going to give you 3550-01, and if you want to refer to it to refresh your recollection, feel free to do so, okay?

A. Thank you.

Q. You also told them, when they asked you, if you had -- you said to them that you had seen no alerting behavior from Mr. Schulte. Correct?

A. I don't see this in the highlights.

Q. Okay. Do you recall telling them that while you thought

Mr. Schulte might have been unhappy or disgruntled, that there was no other behavior that you saw that concerned you?

Take a look at page two, would you, the second paragraph. I may have forgotten to highlight it. It is the third line.

A. Yes, I see it.

Q. Okay. So you recall now saying that to the FBI?

A. It's in this document, yes.

Q. And the document is a writeup of a meeting with you, right? If you take a look at the front page.

A. Yes, this seems to be a summary of our -- of my meeting with the FBI.

Q. Okay. They asked you, did they not, the FBI, about Mr. Schulte's foreign travel?

A. I don't remember.

Q. And is it fair to say that you knew Mr. Schulte not to be a good traveler?

A. Or he didn't like to travel?

Q. Foreign travel.

A. Right.

Q. You told them that he wasn't big on foreign food or foreign travel?

A. Right, he didn't like it. But how good he is at it, I don't know.

Q. Fair enough. But you told them he didn't like foreign

travel, right?
A. That is a true statement. I don't know if -- I don't remember saying that.
Q. Okay. You know it to be true also that you think Mr. Schulte was reliable, correct?
A. Yes.
Q. And thought he was hard working, correct?
A. Yes.
Q. And is it fair to say that you told the FBI that you and others at the CIA had talked about the Snowden incident, correct?
A. Me and co-workers did talk about the Snowden incident, yes.
Q. You told the FBI, did you not, that when the Snowden incident occurred, everyone at the FBI talked about how that could also happen to Confluence, correct?
A. At the FBI?
Q. I mean at the CIA.
A. At the CIA, yes.
Q. You all talked about it, right?
A. I don't remember if we specifically mentioned Confluence. But we definitely said something like this could happen here.
Q. Take a look at page three of three, would you. See if that refreshes your recollection that you said people at EDG said the same thing could happen to Confluence.
A. Do you have a paragraph?

Q. Sure. Page three, second paragraph, last line.
A. Yes, I see it here.
Q. Right. Do you recall Mr. Schulte telling you that he had quite a few expletives about Mr. Snowden, and he thought he was a traitor?
A. Yes.
Q. You also told the FBI, did you not, that access to DevLAN was, I quote, broad.
A. Sorry, can you repeat the question?
Q. Sure. Broad, B-R-O-A-D.
A. I don't remember saying that. But, yeah. People -- as long as you were a developer, you could get access to DevLAN.
Q. Could you put that piece of paper, you can set it aside. There you go.
Did the FBI insinuate to you at that time that because Mr. Schulte was unhappy or disgruntled at the CIA, he would be the person who would have done this?
A. I don't remember these meetings. They're very -- they're very blurry. But, it was clear that they had an interest in him because of all the things that had happened prior to him leaving.
Q. Is it fair to say that others at the CIA also thought that, because he was unhappy at the CIA, he would be the one to do this?
A. I think that was the general assumption.

Q. Right?
A. I can't think of anyone in specific that told me that, but, I feel like there was that feeling, yes.
Q. Right. And that assumption was passed on to the FBI every time the FBI interviewed anyone at the CIA, correct?
A. I don't know what the other interviews went like.
Q. Okay. When the FBI was interviewing you for the first time, they asked you about Mr. Schulte's family, correct?
A. I don't remember.
Q. You don't remember them asking you if you'd ever met his parents, his mother and father?
A. Yeah, I don't remember that specific question.
Q. It's on the handwritten 302 on page two of six.

Do you by any chance remember telling them that you had not met his parents, but that you knew he was from Texas?
A. I don't remember the specific questions, but that is a true statement.
Q. Just go to page two. And then you told them, did you not, that as far as you knew, Mr. Schulte liked the United States government, correct?
A. I don't remember saying this, but that's true, yes.
Q. Right. And you told them that, in fact, what he wanted to do was to kill the terrorists, correct?
A. I don't remember saying this, but, he -- he definitely had some colorful things to say about terrorists.

Q. And he also told you repeatedly, did he not, that in his opinion, America was the best country?
A. Yes.
Q. And the FBI asked you if you knew Mr. Schulte to attend any rallies or protests; do you remember that?
A. I do not remember that.
Q. Okay. Do you recall Mr. Schulte -- take a look on page four of six, okay, the first full paragraph, the last line.
THE COURT: What's the exhibit number you're working with?
MS. SHROFF: I'm working with, your Honor, 3550-03, page four. Do you have it?
THE COURT: I've got it, thank you.
Q. Does that refresh your recollection?
A. Yes, it's stated here in the document. I can't read that last line.
Q. "No rallies or protests" is how I read it.
A. Right. No rallies or protests. And that's true, I still to this day don't know of any rallies or protests that he attended.
Q. Then they talked to you about your involvement in helping him move from Virginia to New York, correct?
A. Yes.
Q. They asked you a whole series of questions as to how you came about to help him move, correct?

A. Yes.
Q. And they asked you why you helped him move, correct?
A. I don't remember specific questions, but I do remember questions about helping him move.
Q. And you explained to them that it was like a coincidence, right? You'd already planned a trip with another friend, he was moving at the same time, he needed help loading up luggage and moving stuff, correct?
A. Yes.
Q. It was not preplanned, right? It just happened, right?
A. Yeah.
Q. You told them that you had already planned to do this with another friend, right?
A. Yes.
Q. And then they asked you about that friend, correct? They asked you what the name of the friend was, correct?
A. Yes.
Q. Then they asked you for your friend's number, correct?
A. I don't remember specifically what information they asked for.
Q. We'll come back to that if we need to. Let's move to the next point.
They then asked you if Mr. Schulte had left any stuff with you, correct?
A. Yes.

Q. You told them that he had, correct?
A. Yes.
Q. It was normal, everyday stuff he left with you, correct?
A. I wouldn't say it's normal. It was a lot of furniture. So I don't think that's normal.
Q. Oh, to have a -- I agree with you there. But it was furniture, right? It was nothing unusual?
A. Right, yeah, the actual things were not unusual.
Q. Okay. And he had a lot of servers in his house? You visited his house in Virginia, right?
A. I did visit his house. He had a lot of computers.
Q. He played a lot of League of Legends or something?
A. Yes.
Q. Some kind of game?
A. Yes, it's a video game.
Q. A lot of men, people play it; is that right?
A. It has a large user base.
Q. It is some kind of online game where you pretend to have avatars and kill each other online or something like that?
Is that right, basically?
A. Yes.
Q. And you played that game, did you not, with Mr. Schulte?
A. Yes.
Q. And then there was some other cousin of his, Mr. Miller, Justin Miller would played that game, correct?

A. That's not a cousin of his.
Q. Is that somebody who played another game with him?
A. Yes.
Q. And somebody named Shane who played that game with all of you?
A. Yes.
Q. And you all went online with your little headset and played that game after work, correct?
A. Yes.
Q. You told the FBI that he had a lot of servers in his home, correct?
A. I don't remember specifically saying that.
Q. Okay. And at that point in time during that interview, do you remember if they asked you about your use of Confluence? Do you remember if they asked you?
A. I think so, yes.
Q. How about your use of Stash?
A. I don't remember.
Q. How about Jira?
A. Yeah, I think the questions were broad about the Atlassian suite. I don't know if they got into specific ones. Maybe they did.
Q. Let's turn to your next meeting with the FBI which was on June 8th of 2017, okay. This is your second interview with them, right? And at this time, they are still just simply

asking you questions, correct?
A. I don't remember the second meeting.
Q. I'm sure you don't. Trust me, it's been a while, so I understand that completely.
But you met with them a second time, right?
A. Yes.
Q. And again during that meeting they didn't ask you about any other person other than Mr. Schulte, correct?
A. I don't know.
Q. You don't know?
A. I don't remember.
Q. Okay. Let's give you 3550-04, and I think I highlighted for you so it will go easier.
A. Thank you.
Q. It was during this meeting that you told them about Mr. Schulte reaching out to you after the leaks had become public; correct? Do you remember that?
A. I remember telling them about him reaching out to me. I don't remember if it was this specific meeting.
Q. Okay. Take a look at the highlighted portion on page one, okay?
A. Okay.
Q. You told the FBI, did you not, that Mr. Schulte had sounded upset to you that people thought it was he who had done the leaks, correct?

A. Yes. I believe the word was he seemed concerned.
Q. Right. You would be concerned too if somebody accused you of something you didn't do, correct?
A. Yes.
Q. And you also told them that you essentially blew him off, correct? You didn't want to engage and talk to him, correct?
A. Yes, I ignored the initial text messages. And then in the phone call, I didn't want to talk about that subject.
Q. Okay. And at first you didn't report the fact that Mr. Schulte contacted you, correct?
A. Correct.
Q. And then somehow or the other, the deputy chief of EDG said if somebody's contacted you, report it. And then you reported it, correct?
A. Correct.
Q. Now, during this meeting, do you remember if the FBI showed you any documents?
A. I don't remember --
Q. Okay.
A. -- at which meeting they showed me documents.
Q. But there came a point, did there not, that they showed you -- let me just show it to you right now, 3550-503, and it is a three-page document that consists of photos.
A. Thank you.
MS. SHROFF: Your Honor, the government agrees to

introduce it as evidence as Defense Exhibit F.

THE COURT: F is received in evidence.

(Defendant's Exhibit F received in evidence)

MS. SHROFF: Could you pull it up for the jury.

Q. Do you recognize this?

A. Yes.

Q. And you recognize this to be what, sir?

A. This is a screenshot that the FBI showed me during one of our meetings.

Q. You see the date on top?

A. On top of the screenshot or right beneath the title?

Q. No, no. Right there, 6/01?

A. Yes, I see it.

Q. And that's during your June 1st, 2017, meeting with the FBI?

A. I don't remember when they showed me these documents.

Q. Fair enough. And you agreed that this is Mr. Schulte's login page, correct?

A. Yes.

Q. Desktop of a virtual machine, correct?

A. Yes.

Q. Josh's DevLAN screen, correct?

A. No.

Q. No, it's not correct? What is it then?

A. This is a VM that he would have run on his DevLAN machine.

Q. So it is a virtual machine that he ran on his own DevLAN, correct?
A. Yes.
Q. Okay. So it says "Josh." Correct?
A. Yes.
Q. Then it says "Michael," correct?
A. Yes.
Q. And then it says "other," correct?
A. Yes.
Q. And they asked you about this document, correct?
A. Yes.
Q. And you told them, did you not, that Josh had given you what you turned as a phrase "pseudo creds," correct?
A. I don't remember specific wording but, yes. I believe he gave me pseudo accesses to this VM.
Q. Just if you need help, it's on page two of the document I showed you before. Okay?
A. Okay.
Q. And then you told them that you probably had root access to the machine to do with it what you wanted, correct?
A. Yes. If I had pseudo creds, then that's true.
Q. They asked you if you were surprised to find out that you shared a VM with Josh, and you said no, correct?
A. Correct.
Q. Right. And you told them that it was normal to do this at

the CIA, correct?
A. To do it in -- to do it in AED, at least, it's normal.
Q. I'm only talking about where you were, sir.
A. Right. CIA at large it would be very --
Q. You know, that's a fair point. Just in your group that you were working with Mr. Schulte.
A. Right.
Q. At that time.
A. Yes.
Q. So in that group, it was very normal. You tried to explain this to the FBI, correct?
A. Yes.
MS. SHROFF: You can take that down.
Q. Then you told them also why it was normal, correct?
A. I don't remember but --
Q. Okay. Let me see if I can help you remember. You said it was normal to share, because you worked on operations together, and everyone in the branch helped each other with their tools, correct?
A. That's a true statement.
Q. And then you kind of added that it kind of sucked that your name was on this VM, correct?
A. I don't remember that.
Q. Take a look at the first paragraph, page two of eight. It sucks. I don't mean to be rude, but that's the word it says,

"suck," right?
A. Yes.
Q. That your name was on the virtual machine, correct?
A. Correct.
Q. And that you understood from the FBI that that put you under the microscope, correct?
A. Correct.
Q. Then you also tried again to explain to the FBI, did you not, that there was nothing nefarious about this, right? That this was normal to have a VM, correct?
A. Yeah, it says that here.
Q. Right. And that you told them again that this is just part of the work you guys did, right? You shared VMs?
A. Yeah.
Q. Okay. And then, that's the word you used "nefarious," that there was nothing nefarious about this, right?
A. That's the word that's in this document, yes.
Q. Okay. Now, they asked you, did they not, in great detail about what projects you worked on with him, correct?
A. It does say so here, yes. I mean, I don't see that specific question, but it goes on to talk about projects we worked on.
Q. Right. Is it fair to say, sir, that when you were talking to them, there was a lot of stuff you didn't remember even back then, right?

A. Right.
Q. And then you told them, look, if you want, I can follow up and get you the answers, because they seemed to be really interested in these answers, correct?
A. I do remember following up, yes.
Q. Right. And then when you told them you could only remember two projects, they told you to follow up with them and give them the names of the other projects, correct?
A. I'm sure it says that here.
Q. Okay. But it would be a normal thing, right? If they asked you something you couldn't remember, you said, "I'll follow up and give it to you," right?
A. Yes.
Q. Now, during this same interview, which is still June of 2017, seems like a very long interview because it's -- but they asked you about the use of hard drives, correct?
A. I don't remember.
Q. Take a look at page two, second-to-last paragraph. Penultimate paragraph over there. It starts with "later."
A. I see it.
Q. Then they asked you of all things about hard drives you had bought for him on Amazon. Do you remember that?
A. I do.
Q. Right. And you explained to them that it was perfectly benign that you bought hard drives for him on Amazon, correct?

A. In this specific case.
Q. Right. We're only talking -- was there ever a case where you bought him hard drives that you did not think was benign?
A. I only ever bought him hard drives this one time. But the reason, like, I wouldn't normally just buy him hard drives, I would have told him to buy it himself. But the reason was there was some deal going on, and so he's like, if I buy it and then you buy it, we all get the deal and I'll just pay you back.
Q. Right. It's normal, right?
A. Yeah.
Q. Yeah. Amazon had a cap on the sale, like everyone could only get two, and he wanted four or something like that?
A. Yes, it was something along those lines.
Q. I want to make sure I understand this. You told the FBI that when Mr. Schulte asked you to buy these hard drives for him, he gave you his credit card so that the purchase would be tracked to his credit card, correct? Take a look at that paragraph. You see that?
A. Yes.
Q. Okay. And then also the hard drives were actually delivered to Mr. Schulte's house. It's not like they came to your house and then you gave them to Mr. Schulte, right?
A. Correct.
Q. Right. Okay. They had brought with them a printout of

the Amazon purchase, correct? Do you remember that?
A. The FBI?
Q. Yeah.
A. No, I don't remember that.
Q. Okay. Do you remember that during this interview, they made you drive off site so that could you pick up your e-mail and show them this Amazon purchase on your e-mail?
A. I remember driving off site to show them things. The e-mail could have been one of them.
Q. Okay. And during this interview, they covered topics that they had covered already. They re-covered the fact that you helped him move to New York, correct? Just flip the page over.
A. Yes, I see that here.
Q. Okay. And then you gave them all of the details again as to how you came to share a ride and went to New York with him, correct?
A. Yes.
Q. And again, there was nothing nefarious about that at all, correct?
A. Correct.
Q. Okay. And then you told them that you had spoken to him since he had started work at Bloomberg, correct?
A. Correct.
Q. And that he had told you, and then you had told the FBI, that life at Bloomberg was good, correct?

Take a look at three of eight at the bottom. It's highlighted.

Do you recall him telling you he found his new job interesting, correct?

A. Yes, I said that.

Q. He joked about how he thought it was kind of cool for him to be at Bloomberg and be known he had worked at the CIA?

A. I do remember him mentioning that being on his profile.

Q. He told you, right, that he missed the mission, he didn't have a lot of friends in New York yet, but he was doing okay at Bloomberg, right?

A. Yes, I remember the not having a lot of friends in New York yet.

Q. He had just moved here, correct?

A. Yes.

Q. And anyway, like many other developers, he had a hard time making friends, correct?

A. Yes.

Q. The FBI asked you about Mr. Schulte's financials, correct?

A. Do you have a cite? I don't remember a specific question about his financials.

Q. Okay, I'll make it easier. Do you recall them asking you if he ever used bitcoin?

A. No, I don't recall.

Q. I'll get to that in a minute. But as far as you knew, you

never saw Mr. Schulte live above his means, correct?
A. No.
Q. And then they spoke again about the security about DevLAN, correct?
A. Do you have a cite? I don't remember a specific question.
Q. Take a look at page four. Let me move forward from that.
A. Okay.
Q. And then they talked -- they asked you about his relationship or his impression of Karen, correct?
A. Of caring?
Q. Karen. K-A-R-E-N, Karen?
A. Oh.
Q. Do I have that name wrong?
A. I don't remember that question. I thought you said the word caring, C-A-R-I-N-G, and I didn't remember that question either.
Q. Do you see -- does that remind you?
A. I don't remember a question about Karen.
Q. Okay.
A. I see it at the bottom.
Q. Take a look at five of eight. Do you see the top paragraph on page five?
A. Yes, I see that, the last two sentences of page four and pulls over to page five.
Q. Right. And he told you, did he not, that he thought she

was just trying to get promoted, correct?
A. I remember that his sentiment of Karen was she was not taking his report seriously.
Q. Right. And she was just trying to get promoted, correct?
A. I don't remember him specifically saying that, but I know he thought she was not taking this seriously, just wanted to ignore this, and just wanted this to go away.
Q. Does it not refresh your recollection about trying to get promoted? You see it's crossed out by the line?
A. Oh yeah, I wasn't looking at that because it's crossed out.
Q. It's just he typed it too close to the line.
A. Okay. It does say here to get promoted, so he is willing to go over her head until someone would listen to him.
Q. Right. And he expressed to you his frustration about not being heard by Karen, correct?
A. Yes.
Q. He thought because Karen and Mr. Weber were friends or friendly, she tended to listen to Mr. Weber and not him?
A. Yes.
Q. You told this to the FBI, right?
A. That is a true statement.
Q. And you did your best to explain the dynamics of the CIA to the FBI, because that's what they were asking you about, correct?
A. I answered the questions the best I could.

Q. Right. I mean, you had no control over what they wrote down, but you answered their questions to the best of your ability, correct?

A. Yes.

Q. During the same interview -- you can put that down. You told them about Josh Schulte's love of movies, correct?

A. I don't remember this.

Q. Okay. Is it fair to say he liked movies?

A. Yes.

Q. He had a ton of movies, correct?

A. Yes.

Q. And he had something called movie night?

A. Yes.

Q. He was into getting some kind of Torrent site called "pass the popcorn"?

A. Yes.

Q. I'm not even going to ask you what a Torrent site. It is to watch movies, "pass the popcorn"?

A. Yes, he was passionate about joining this, I don't know this Torrent site.

Q. And when he had these movies, he shared them with everyone at the CIA -- not everyone, I mean in your friend group. Not, you're right, not the whole CIA.

A. Yes. People who wanted access, he would give them access.

Q. Freely, right?

A. Yes.
Q. He never hassled anyone and said, oh, I'm paying for the site, so you pay me. Nothing, right? Just give it to them?
A. Correct.
Q. You remember the FBI asking you if Mr. Schulte was a vigilante hacker by night? Do you remember that phrase they used?
A. I think I do actually, yes.
Q. You told them, no, you didn't know him to be a vigilante hacker at night?
A. Correct.
Q. You in fact did not know him to be a vigilante hacker at night.
A. Correct. I did not know him to be a vigilante hacker.
Q. If you look at page six of 3550-03 is where they ask you if he was ever using bitcoin. And you said no.
A. Do you have the paragraph?
Q. I'm sorry?
A. Do you have the paragraph?
Q. Sure. Let me just help you here.
MR. KAMARAJU: At some point I'm going to ask that the defense counsel stop reading from the document.
MS. SHROFF: Okay.
Q. Put it down, it's okay.
You don't remember that question?

A. No.
Q. That's all right. Do you remember the FBI asking you about Mr. Schulte's use of various software programs, including Tor and Tails?
A. I do remember Tor. They asked if he had used Tor before.
Q. Right. And you told them that he never kept it a secret that he had used Tor before, correct?
A. Correct.
Q. In fact, his group joked about the fact that he used Tor, correct?
A. Yes, him and Jeremy had a discussion about it.
Q. Right. But they also mocked him, correct, like in a good -- I don't mean in a negative way. Just in a joking way, they told him to get off and stop using Tor?
A. Yes. Jeremy said it was -- you were supporting bad things and you shouldn't use Tor.
Q. But Jeremy knew he was using Tor, right?
A. Yes.
Q. And Jeremy -- that's Jeremy Weber, right?
A. Yes.
Q. The man that he and Mr. Schulte didn't quite get along, correct?
A. Correct.
Q. And Mr. Weber thought -- I'm going too fast.
Mr. Weber thought that he should be able to tell

Mr. Schulte what to do, correct?
A. Yes, Mr. Weber --
Q. Mr. Schulte thought that he should not be able to do that, correct?
A. Correct.
(Counsel conferring)
Q. Was it at this meeting that the FBI tried to convince you to wire yourself up and call or text Mr. Schulte?
A. No, they never tried to convince me of this.
Q. Did they ask you?
A. I believe that I had made the statement, you know, I -- I don't remember the specific wording, but I feel like I had actually brought this up, and then at the end of the meeting, they asked me would you do that.
Q. Okay. And you said you would first want to see what proof the FBI had linking Mr. Schulte to these leaks, correct?
A. Yes, I would want -- yes.
Q. And they never followed up after that, right?
A. Correct.
Q. And by the way, was it also in this meeting that they asked you to take a limited polygraph or was that later?
A. I don't remember which meeting that was in.
Q. Okay. We'll get back to that later then. They asked you, did they not, about a meeting that you -- not a meeting, but they asked you about a time that you went into work on a

weekend; is that right?
A. I do remember a question about that.
Q. Right. They had known you had gone in on a weekend, and they asked you about it, right?
A. Yes.
Q. You again explained to them that it was nothing nefarious to go into work on a weekend?
A. Yeah. I don't remember the specific words, but it was normal to go in if you had to get something done.
Q. Right. In fact, sometimes people went to talk about -- to do their PARs, because it's hard to write up a PAR?
A. Yes, specifically I had brought that up and said one of the reasons I come in on the weekend is to do my PAR.
Q. A PAR is a performance -- what is it?
A. I don't know what the acronym stands for. Something about our performance review. It's how you -- you write up how you think you've done for the year.
Q. Personal Appraisal Review maybe?
A. Something.
Q. Something like that?
A. Yeah. It's your push for promotion.
Q. Okay. And at first you thought that you had gone in to write a PAR, correct?
A. Yes.
Q. But then you realized you'd actually gone into work on a

project, correct?
A. Yes. Well, this is one of those where I said, you know, my best guess is I came in to work on my PAR, but I will follow up with you. I save all my PARs so I went, looked at the time stamps on the PARs, none of those were during that date. So then I went back to other, we had to fill out these weekly activity reports that say kind of what we did for the week, so I looked at that. And I was like I must have been working on this project.
Q. Right. And you followed up, you did all of that, and you told that to the FBI, right?
A. Yes.
Q. They asked you about that weekend because Mr. Schulte also happened to be working that weekend?
A. They mentioned that, yes.
Q. Did you think it was odd that Mr. Schulte was working that weekend or did the FBI think it was odd that Mr. Schulte was working that weekend or both?
A. At first I thought it was odd.
Q. Okay.
A. Just because --
Q. Go ahead.
A. Just because, you know, although it was normal to come in on the weekend, it was less common -- rare, I would say, to come in on the weekend. One of us probably would have told

each other, you know, we were going to come in on the weekend.

But then I looked at my situation, I was like, well, I didn't tell him I was coming in, so I guess this is normal.

Q. Okay. You told that whole story to the FBI, right?

A. I don't remember.

Q. You met with them again after that. That meeting was June, then you met with them in August, right? August 30, 2017?

A. I don't remember the date.

Q. That's fine. And I just want to make sure that the record is clear. At that time you're not on administrative leave, right? You're still a full-time CIA employee?

A. Correct.

Q. And again, they asked you a whole slew of questions, correct?

A. Yes.

Q. And it is in this meeting, if you remember, that you told the FBI that, in your opinion, Mr. Weber was setting Mr. Schulte up. Do you remember that?

A. I remember feeling that way.

Q. Okay. By that you mean that you thought Mr. Weber was setting Mr. Schulte up to fail at his job at the CIA, right?

A. I thought he was -- baiting him into using his accesses, for a lack of a better word.

Q. Did you say "baiting"?

A. Yes.

Q. B-A-I-T-I-N-G?
A. Yeah, I thought he was setting -- he was creating circumstances where he knew that Josh had access to change permissions on the server, Josh was an admin. He was telling Josh you cannot do this. But Josh technically could do that, right, he had the technical capability to do that. So, Josh was going to do that.
Q. Okay. You told Mr. Weber your concern?
A. Yes.
Q. And Mr. Weber said butt out, correct?
A. Yes, in summary. Mr. Weber said butt out.
Q. By then Mr. Schulte had actually confided in you -- he confided in you, you were friends, right?
A. Yes.
Q. He told you, right, that he felt hassled by that memo of warning, correct?
A. Yes, yes.
Q. Thought it was unfair, correct?
A. Yes.
Q. And you felt that Mr. Weber was trying to punish Mr. Schulte, correct? That's the word you used for the FBI?
A. I don't remember using that word.
Q. Okay. Did you tell the FBI that you felt that Mr. Weber was trying to punish or stick it to Mr. Schulte?
A. I don't remember saying that.

Q. Did you feel that way?
A. When I think back on it now, I don't know he was trying to punish him as much as -- he just wanted -- he didn't think that Josh should be able to make claims like "I'm the one taking this project" and things like that.
Q. Right. They had a tussle, correct?
A. Yes.
Q. And the tussle was public, correct?
A. Yes.
Q. I mean, Mr. Weber would say things to Mr. Schulte, Mr. Schulte would respond back, and it wasn't like a secret in that cubicle or anyplace else, correct?
A. Right. I don't know that the rest of the division or the rest of the group knew, but definitely within OSB it was known.
Q. And Mr. Weber knew that Mr. Schulte did not consider him, Mr. Weber, to be a person of authority, correct?
A. I don't know what Mr. Weber knew.
Q. Fair enough. Okay. Now, you tried to suggest to Mr. Weber, did you not, that he should tell Mr. Schulte clearly that he was going to remove Mr. Schulte's access from the libraries, correct? Do you remember that?
A. I remember telling him he should -- oh, from the libraries?
Q. You told Mr. Weber that, in your opinion, Mr. Weber should tell Mr. Schulte that he was going to do something to Mr. Schulte before he did it, correct?

A. I remember having a discussion with Mr. Weber saying you should remove his accesses. It's potentially in that conversation I said, you know, and you should tell him as well.
Q. Okay. Let's take a look, shall we, to your -- to a 3550 if you have it there. And that's page 13. 3513, page two.
A. Page two.
Q. I haven't given it to you. Sorry about that.
A. That's okay.
MS. SHROFF: Did you want a copy, your Honor?
THE COURT: Yes, please. Thank you. Great. Thanks.
A. Where am I looking?
Q. Just look at paragraph, there is a paragraph UU and then S. Do you see that, starts with in April. Page two. You with me?
A. Sorry, "in April 2016"?
Q. Yes. Just read it to yourself. Don't read it out loud.
A. Okay.
(Pause)
Q. Let me know when you're ready.
A. Okay, I'm ready. I read the second paragraph.
Q. Does that refresh your recollection that in fact you told Mr. Weber that you thought he was setting Josh up to get into trouble?
A. I remember saying that to him.
Q. And you said that to him, and you said to him you're setting him up, because everybody knew how Josh would react,

correct?
A. Yes.
Q. And then you said to him that -- you were kind of even Steven, right? You also told him that you thought Josh should calm down, right?
A. Yes.
Q. And then you said that he should really -- by "he" I mean Mr. Weber -- should really tell Mr. Schulte before removing his accesses that he was going to do so. Correct? That was your opinion, correct?
A. Yes, yes, it does say that here.
Q. Right. And then you also said to the FBI that back then when you were not on administrative leave, it was your belief that Mr. Weber was trying to punish Mr. Schulte and trying to get him to violate the letter he had signed about not abusing his privileges. Do you see that? I highlighted it for you.
A. Yes, I see it.
Q. Okay. You can put that aside.
You know of a project called Brutal Kangaroo, correct?
A. Yes.
Q. Do you remember telling the FBI in the same interview that Brutal Kangaroo was a complex tool?
A. I saw that in that paragraph.
Q. Right. And it was in fact a complex tool, correct?
A. Correct.

Q. And is it fair to say that in your opinion, at least, nobody in OSB wanted to work on it?
A. Yes.
Q. Okay. But Mr. Schulte was open to working on it, correct?
A. Yes.
Q. In fact he wanted to work on it, correct?
A. He was the creator.
Q. I'm sorry?
A. He was the creator.
Q. He was the creator of Brutal Kangaroo?
A. Yes.
Q. Right. And nobody else wanted to work on it but he did, correct?
A. Yes.
Q. And you told this to the FBI, and then you also told the FBI that you did not think Josh would do anything to hurt the agency, correct?
A. I don't recall. I remember telling them he wanted to work on at it, I see that in here. I don't remember seeing the whole agency thing.
Q. Okay. We'll find it in a minute.
A. Okay.

(Continued on next page)

BY MS. SHROFF:

Q. Page 3, paragraph 2.

MS. SHROFF: Thank you.

A. What does the paragraph start with? Is it "this screen," or is it --

Q. No. Page 3.

Hold on. Let me just walk to you.

It's item No. 1.

A. Item No. 1.

Q. Yeah.

A. I saw No. 2, and I just went down to that.

MS. SHROFF: Do you have some water up there, sir?

THE WITNESS: I do not, but I'm OK.

Thank you.

MS. SHROFF: Thank you.

Q. Do you see that phrase that you "did not think K.P. would do" -- I'm reading, "that Mr. Schulte would not do anything to harm the agency," correct? Does that refresh your recollection?

MR. KAMARAJU: Your Honor, we object to the reading again.

THE COURT: Yes. You can't read from a document that's not in evidence.

MS. SHROFF: I'm sorry. I can highlight it for him.

THE COURT: Yes.

A. I know you pointed this out to me. I just don't see it. I'm sorry. Can you point it out to me?

Thank you.

Yes, it says that. One.

Q. Do you see that?

A. Yes.

Q. You told them that, right?

A. Yes.

Q. And then again in that interview, they covered with you this issue of the screenshot that Mr. Kamaraju showed you on direct, correct?

A. At some meeting I remember them discussing the screenshot.

Q. All right. I'm going to try and heed the admonishment and not read from the document, so you read and see if that refreshes your recollection.

A. Yes, I see it down here.

Q. OK. So they talked to you about this screenshot, correct?

A. Correct.

Q. And they asked you a lot of questions about it, correct?

A. Yes.

Q. They asked you when you had taken that screenshot, correct?

A. I don't remember the specific question, but I'm sure they did.

Q. OK. And how many screenshots do you recall them showing you?

A. I think three.

MS. SHROFF: OK. Can we just pull them up, please. 155.

Q. OK. So these are the three screenshots they showed you, correct?

A. I counted this as one screenshot.

Q. Oh, OK.

A. In addition to the ones you just showed me earlier.

Q. OK. So take a look at the one farthest to the left.

A. OK.

Q. They asked you about this screen, correct?

A. Yes.

Q. They asked when you had -- you took -- I just want to make sure.

You took a screenshot, correct? That means, like -- how did you take it, by the way?

A. On the Windows operating system, on the keyboard, there's a print-screen button. If you press that, it automatically puts an image on your clipboard of what's on your desktop.

Q. And you did that, right?

A. Yes.

Q. And you did that on April 20?

A. Yes.

Q. And you, by the way, did not tell anyone about this, correct?

A. Correct.
Q. But you told the FBI about it, or the FBI told you about it?
A. The FBI showed me this screenshot and then asked me if I had taken this.
Q. Is it fair to say, sir, by the time the FBI showed it to you, you had forgotten about the screenshot?
A. Yes.
Q. You had taken it on April 20, 2016, right?
A. Yes.
Q. You forgot all about it?
A. Yes.
Q. You didn't talk to Mr. Weber about it, correct?
A. No.
Q. You didn't talk to Mr. Schulte about it, correct?
A. No.
Q. You didn't talk to anybody about it, correct?
A. Correct.
Q. And then the FBI started to ask you questions about this screenshot, correct?
A. Yes.
Q. They asked you why you didn't tell anybody about it, correct?
A. Yes.
Q. And they asked you what else or what all you did with the

screenshot, correct?
A. I remember questions about this screenshot. I don't remember specifically what I did with it and stuff.
MS. SHROFF: OK. And can you move to the second page, the second part of your --
Q. You're saying this is one, right?
A. This is one screenshot. I had three monitors, so when you hit the print screen, it just takes all of those monitors and puts it together as one screenshot.
Q. Oh, OK. So what does this have to do with anything? What is the second page?
A. What this has to do with anything?
Q. Uh-huh.
A. I believe I was trying to dig into what the screenshot meant. I was unsure. You know, I took the screenshot because I was concerned, and then I tried to validate those concerns by determining did a person do these reverts, or was this a system action? This is me trying to dig into that. I have debug view open to see if there was any debug messages about reverting the VMs or something.
That could have been there already. I don't know. But specifically this command prompt here that you see, this black-and-white text, the command prompt, I was looking at IP addresses.
Q. And did you do that on the same day, or you did this later?

A. No. Same day.

MS. SHROFF: OK. And let's move to the third part.

Q. This is also what you took, right? This is your third of your three screens, right?

A. This is the right side, yes, of my screenshot.

Q. So you didn't tell anybody about any of these three shots, correct?

A. Correct.

MS. SHROFF: Can I go back to the first one, please.

Q. Now, you see all the way at the bottom, this is on a vSphere, correct?

A. Yes.

Q. Were you running the vSphere the whole day of April 20, or you don't recall anymore?

A. It was very typical for us to just have this thing open for days.

Q. For days, right?

A. Yes.

Q. So is it your testimony that -- you see the timing at the bottom?

A. Yes. The start time?

Q. Yeah.

A. Yes.

Q. And you don't see anything before the start time of 6:55?

A. Yeah. I don't see anything before 6:55 -- or I see 6:51.

Q. Right, but you're saying that even though your vSphere was running, you didn't see any April 16 snapshot?
A. Yeah. I don't see an April 16 snapshot.
Q. And sitting here, you don't remember seeing an April 16 snapshot, right?
A. Correct.
Q. Sitting here today, you don't remember how long this thing had been running; it could have been running all day, and that's common you already said, correct?
A. Correct.
Q. How many other people are running vSphere?
A. It was a common tool for the team to use.
MS. SHROFF: OK. You can take that down.
Q. Now, you said that it's common for people to remain logged in to vSphere, correct?
A. Yes.
Q. Is it also common for people to remain logged in to DevLAN?
A. Yes.
Q. Is it common for people to stay logged in to the Same Time chat thing?
A. No.
Q. OK. It's not common?
A. No.
Q. You log out of that one, right?
A. Same Time?

Q. Yes.
A. Yes, we log out of that one.
Q. Now, the screenshot that Mr. Kamaraju showed you and the FBI showed you back then, you didn't talk about it with Mr. Schulte?
A. Correct.
Q. You certainly didn't talk about it with Mr. Weber?
A. Correct.
Q. How about Karen?
A. No.
Q. Now, the FBI asked you repeatedly if you'd ever seen Mr. Schulte carry hardware in or out of the CIA facilities, correct?
Take a look at page 4. If you don't remember, take a look. If you remember, just answer, please.
A. I don't remember the specific question. I'm looking for it in the document.
Q. OK. Well, let's just start this way. You had never seen him walking in and out with hard drives, correct?
A. Correct.
Q. And do you remember them asking you if Mr. Schulte ever used something called a throwaway email account?
A. I don't remember the specific question.
Q. OK. Well, if they did ask you that question, would you have said you do not recall him ever using any throwaway email

accounts?
A. I -- if I would have said that, I would change my opinion.
Q. OK. You would change your opinion now --
A. Yes.
Q. -- you're saying?
A. Yeah.
Q. But did you know him to use any throwaway email accounts?
A. It was common if we needed to register for, like, a free site to use a throwaway email.
Q. What is a free site?
A. Like, if you need something online, like -- I'm having a hard time thinking of something, but let's say I needed, like, a code. Like, let's say there's a website that hosts code, examples of code. Like, I want to copy this file, and this website says, Hey, we have something that does that for you, but you have to sign up for free to get that code sample. We would use that throwaway account email to sign up to that website and get the code sample, or do whatever it was.
Q. It's kind of like when you want to get something free and you sign up --
A. Right.
Q. -- with an account, but you don't want to get those, Hey come shop with us more?
A. Right, right, right.
Q. That's called a throwaway account?

A. Yes.
Q. That's a normal thing to do, right, in your business?
A. Yes.
Q. And everybody at the CIA had that type of CIA account?
A. I don't know about the whole CIA.
Q. And when I say the CIA, I just mean in your group.
A. Yes, certainly in my group that was a common thing.
Q. And you and he were in the same group, correct?
A. Yes.
Q. Do you recall them asking you if you ever used a spy pen?
A. I do not recall that.
Q. Now, is it in this interview, do you recall, if they asked you if you would undergo a limited --

MR. KAMARAJU: Your Honor, could we have a sidebar?

THE COURT: Yes.

(Continued on next page)

(At sidebar)

MR. KAMARAJU: Thank you.

I believe where Ms. Shroff is about to go with this question is to ask whether the FBI asked him to undertake a polygraph exam. We have briefed extensively the idea of polygraph exams being inadmissible. Your Honor ruled, in a very narrow circumstance, some information about the defendant's polygraph could come in, and the Second Circuit has been very clear that polygraphs were exactly the purpose that she's trying to introduce it -- sorry; I apologize -- that polygraphs for the purpose of impeaching a witness are not admissible.

THE COURT: Why did the government ask for it then? Why did the government at the time ask for the polygraph? Usually it's the defendant who says it's unreliable. Here, it's the company, the CIA, or the FBI, that says it's unreliable. Why isn't that the best of both worlds. You get the polygraph and you get it accepted or rejected depending upon the results. I don't understand the objection. I don't think it's well-taken.

MR. KAMARAJU: Your Honor, whether we asked for the polygraph or the defendant asked for the polygraph, the question is whether you're going to get into the reliability of polygraph examination.

MS. SHROFF: Your Honor, I'm going to make it easy for

Mr. Kamaraju. I'm just going to point out that the FBI asked him to take a polygraph and he said no. There's nothing about reliability here anyway.

THE COURT: OK. That ends it. Thank you.

(Continued on next page)

(In open court)

THE COURT: All right. Ms. Shroff.

Q. They asked you to take a limited polygraph?

A. Yes, at some point they did.

Q. And you declined, correct?

A. Yes.

Q. OK. Let's turn to your April 28 -- you can put that document aside.

You next met with them in April of 2018. OK?

A. OK.

Q. And again, they asked you a lot of questions that are repetitious, so I won't repeat them here, but do you recall if they repeatedly asked you about this League of Legends game? Do you recall that, or no?

A. No.

Q. They asked you about your friendship, and you explained your friendship with Mr. Schulte to the FBI, is that correct?

A. Yes.

Q. You explained that you went to lunch together, correct?

A. Yes.

Q. He had this weird habit of putting a potato in the microwave and keeping you waiting before you went to the cafeteria, correct?

A. I thought that was normal, but that is true.

THE COURT: There you go.

Q. You explained to them that you went to the gym with him, correct?
A. Yes.
Q. And you explained to them the nature of the relationship, that you were friends, correct?
A. Yes.
Q. And again, they focused on the fact that you and he -- or at least he had initiated contact with you after the leaks, correct?
A. That is correct.
Q. Right. And that he had also texted you as part of that, correct?
A. Yes, he texted me.
Q. Right. And when he texted you, he used his own phone, correct?
A. Yes.
Q. He didn't refer to himself as anybody but Josh Schulte, right, or as Josh?
A. Yeah. He didn't -- I just knew it was him because his phone number was saved in my phone.
Q. It's the same phone number from before, right?
A. Yes.
Q. OK. They again asked you to talk to them about projects that were worked on on thumb drives outside of the office and brought into the office. Did they ask you about that; do you

remember?
A. I vaguely remember a question about -- I don't remember the whole thumb-drive thing but a question about projects worked on outside of the office.
Q. And one such project was Project Whiz. Do you remember that project?
A. No.
Q. OK. But it's fair to say that people worked on a part of the project outside of the CIA facility and brought it into the facility, correct?
A. What was the question? Is it common?
Q. Yeah. People do that, right? I mean, I don't know how common, but do people do that?
A. It was done. I would not say it was common.
Q. OK. But it was done, right?
A. Yes.
Q. And you told the FBI that, right?
A. I don't remember.
Q. OK. Take a look, if you want, at 3550-17. But you also did tell the FBI that it was a one-way street; people didn't take any work they did at the CIA outside the CIA, correct?
A. Right, I remember saying that, yeah, if you're going to do a project outside, it comes inside, and then that's it; it stays here.
Q. This one is easy.

A. One paragraph.
Q. The last page, and the only question is, does that refresh your recollection?
A. This doesn't mention the outside projects. It just --
Q. Take a look at the last line. No?
A. Yup, it is there. I'm sorry.
Q. OK. Does that refresh your recollection, the last line, that you told the FBI that?
A. Yes.
Q. OK. Now, you're still fully employed at the CIA at that time, right?
A. Yes.
Q. OK. And then the next meeting you have with the FBI is on August 16, 2019; yes?
A. I don't remember the date.
Q. OK. And at this meeting, you have two prosecutors present and an FBI agent present. Does that ring a bell for you?
A. Uh, I don't remember who -- I feel like my first meeting where there were prosecutors, there was more than two, but I don't know for sure.
Q. Well, is this the first time you've met Mr. Kamaraju, do you think?
A. I don't remember the date I met him. At some point I do meet him for the first time.
Q. OK. And do you recall that during this meeting they again

told you that you had to be truthful? Correct?
A. I don't remember. But I do remember at varying points they told me I had to be truthful.
Q. Right. And in this one, they actually told you that you could have an attorney present if you want, right?
A. I don't remember.
Q. OK. Let me see if I can give you -- I'm going to give you a document that ends with 027640.
A. Thank you.
OK. I've read the bullet points.
THE COURT: What's the question, Ms. Shroff?
BY MS. SHROFF:
Q. So, this is the meeting at which you are advised, if you want, you can have an attorney, correct?
A. Uh, yeah. I think from the get-go, from my very first meeting, they told me, you know, you have a right to have an attorney. I don't think this is the first time I'm hearing this.
Q. OK. So this doesn't strike, this meeting doesn't stick out in your mind as anything different from any other one?
A. No. It does.
Q. It does, right?
A. Yes.
Q. OK. We'll get to that in a minute.
And in this meeting, they explained to you, did they not,

the difference between being questioned by the Department of Justice and being questioned by the CIA people, correct?
A. I don't remember, like, a lengthy distinction between the two.
Q. OK. Do you remember them trying to explain to you that lying to them was a crime?
A. I don't remember that, but I do remember them at some point saying you have to be truthful, truthful to us; it's a crime not to be.
Q. OK. And at this meeting, they started substantively talking with you about the screenshot that you had taken, correct?
A. Yes. I see these -- I see that in the bullet points.
Q. OK. And then they asked you again, or at least they started discussing with you the fact that you had told them that you didn't remember taking that screenshot, correct?
A. Correct.
Q. And you again emphasized to them that you just didn't remember taking that screenshot, correct?
A. Correct.
Q. You just didn't remember taking it on April 20, right?
A. Right.
Q. And you told them that you hadn't talked to Mr. Weber about that screenshot; you told them this again, correct?
A. Correct.

Q. And you told them, did you not, that one of the reasons you didn't talk to Mr. Weber is because you had tried to talk to Mr. Weber before but he had blown you off, correct?
A. Correct.
Q. You tried to explain that to the FBI and the prosecutors, right?
A. Yeah. Specifically he said stay out of it.
Q. Right. He told you to stay out of it, right?
A. Yes.
Q. Mr. Weber did?
A. Yes.
Q. And you told them that you had -- I mean, I don't know if you used the word "investigated" but that you had investigated the snapshot, right?
A. Yes, I had looked into it.
Q. And that you had investigated to see if that account was accessing or using or missing logs, correct? Do you see that? Look at the last bullet. Just read that whole bullet.
A. "M. investigated the snapshot to see why" --
Q. Don't read from the document.
THE COURT: Don't read aloud. Just read it to yourself.
THE WITNESS: Oh, I'm sorry.
BY MS. SHROFF:
Q. Just read it to yourself.

A. OK.
Q. Now, you'd already talked to them many times, correct?
A. Yes.
Q. OK. And you explained to them that you didn't see any logs, and then you tried to explain to them why it was -- what the reason was why you may not see logs and that could be logical, correct?
A. Yes. There could have been a good reason why that account could not see the logs.
Q. Right. And that's because you had one kind of account, and another kind of account would be needed to see the logs?
A. Yes, there's potential that the server was set up in such a way where limited -- user accounts could not see the logs whereas a full administrator account could.
Q. Right. And you explained that to them, right?
A. Yes.
Q. And then you told them that you were not sure that it was Mr. Schulte who had done the reversions on April 20, correct?
A. Correct.
Q. And after you said that, they stopped the interview, correct?
A. At some point they stopped the interview, yes.
Q. Right. And then you asked for a lawyer, correct?
A. I believe I asked for a lawyer before they stopped the interview.

Q. Fair enough. You asked for a lawyer and they stopped the interview, correct?
A. Yes.
Q. And at that time when you told them that you did not believe that Mr. Schulte had done the reversion, you were still a full-time employee at the CIA?
A. Correct.
Q. OK. And then that interview ended. By the way, where was that interview?
A. Where was it?
Q. Yes.
A. It was here in New York.
Q. I'm sorry?
A. Here in New York.
Q. Oh, it was in New York?
A. Yes.
Q. OK. And the interview ended, right?
A. Yes.
Q. And then you left?
A. Yes.
Q. And did there come a time after the interview ended that you went ahead and got yourself a lawyer?
A. Yes.
Q. And you hired a lawyer, Ed MacMahon, right?
A. Yes.

Q. Do I have his name right?
A. Yes.
Q. And the prosecutors had told you to have your lawyer call them, correct?
A. Yes.
Q. And you had Mr. MacMahon -- you retained Mr. MacMahon, correct?
A. Yes.
Q. He's a well-known criminal defense lawyer, correct?
A. Yes.
Q. Well-known for representing people who are accused of wrongful conduct with leaks, right?
A. Yes.
Q. And you hired him and had him call them?
A. Yes.
Q. And right after this, is that when you learned that you were put on administrative leave?
A. No. This was before, I, I -- so, right after the meeting, I take a plane from New York back to Virginia, and I, you know, sometime shortly after landing, I get a call from my division chief.
Q. OK.
A. And my division chief said, Hey, come in through this different entrance, and I -- I knew internally what that probably what that meant. My division chief said he did not

know what that meant. So at that point I had a pretty good idea that I was going to be -- something was going to -- some sort of talking-to was going to happen.

Q. Right. But the talking-to had come after this meeting was over, correct?

A. Correct.

Q. And the phone call you got from your division chief was after this meeting was over?

A. Yes.

MS. SHROFF: Your Honor, would this be a good time to take the morning break?

THE COURT: Yes, we'll take our morning break now.

(Continued on next page)

(Jury not present)

THE COURT: OK. You can stretch your legs.

THE WITNESS: Thank you.

(Witness not present)

THE COURT: Please be seated.

I'll see you in 15 minutes.

MS. SHROFF: Your Honor, I apologize. The document we got this morning, I think we're only allowed to read it in the SCIF, so I haven't seen it.

MR. KAMARAJU: We didn't say that, your Honor.

THE COURT: They didn't say that.

MS. SHROFF: Oh, it's marked classified, so I just assumed it was the rule. Can I read it here?

THE COURT: You can read it here. It's in the courtroom.

MS. SHROFF: Oh, OK. My bad.

(Recess)

(Pages 1321-1331 classified and sealed)

(In open court; jury not present)

THE COURT: When I came down this morning, I directed the government produce the attachment to its letter of February 12. I did not direct that the letter itself from Mr. Kamaraju to me, from the government's team to me be produced, because I thought it had been produced. It lists on the cc list defense team by ECF and hand.

MR. KAMARAJU: I apologize.

THE COURT: That's all right. I subsequently directed that the letter be produced as well. And it has been produced now; is that correct?

MR. KAMARAJU: We're having a copy printed right now.

THE COURT: All right. Ms. Shroff, do you have an application? Mr. Zas.

MR. ZAS: Yes, your Honor. At this time, for the reasons we discussed in your Honor's chambers, the defense would move to suspend the examination of this witness and proceed to the next witness, recognizing that there is likely a need to recall this witness to complete both his cross-examination and his redirect examination.

THE COURT: All right. Mr. Kamaraju.

MR. KAMARAJU: We object, your Honor. We think that -- and we are obviously not privy to what defense counsel told you in the robing room. But to the extent --

THE COURT: Just as they were not privy to your

memorandum and the letter that you transmitted the memorandum with.

MR. KAMARAJU: Yes. We appreciate that, your Honor. We're not objecting to fact that they spoke there, I'm just caveating what I'm about to say.

To the extent the argument that they wanted to make, which originally that they articulated was that they want to suggest that the CIA badgered this witness into changing his testimony through putting him on administrative leave. I think Ms. Shroff was about to get there. They have the memo, if they think that advances their point.

THE COURT: You are repeating what you said in your letter, that she's more than adequately prepared for any cross-examination she wants to make.

But this letter discloses something I hadn't seen before, that Mr. Michael might have been a systems administrator. That's what the memo says.

MR. KAMARAJU: First of all, all of the information about his privileges have been disclosed to the defense for years, or months at least, your Honor.

THE COURT: That he is a systems administrator?

MR. KAMARAJU: Yes, your Honor. We produced all the log files to his computer, too. And multiple 302s have said it. That's not a new fact to the defense, your Honor. That's not something that has changed all of a sudden. So, if that's

the basis, then all of that information --

THE COURT: The basis is the late production of this information. I believe it should have been turned over at or about the time that the decision was made. And I think it was not accurate and not correct for you to withhold that information until the witness took the stand.

At any rate, I'm going to grant Mr. Zas's motion. He's going to be continued, continuation of the examination of Mr. Michael.

Do you have another witness available?

MR. KAMARAJU: Yes, your Honor.

THE COURT: Okay. We'll call the other witness.

MR. KAMARAJU: The government calls Michael Berger.

THE COURT: Okay.

(Continued on next page)

(Jury present)

THE DEPUTY CLERK: Please state your name for the record.

THE COURT: Just a minute. I apologize for the long break, not that you're probably too concerned about it. But we had some important legal issues to take up and we're going to resume now with another witness.

THE DEPUTY CLERK: Please state your name for the record.

THE WITNESS: Michael Berger.

(Witness sworn)

THE DEPUTY CLERK: Witness sworn.

THE COURT: Please sit down, Mr. Berger.

MICHAEL BERGER,

called as a witness by the Government,

having been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. KAMARAJU:

Q. Good morning, sir.

A. Good morning.

Q. Are you employed?

A. Yes, I am.

Q. Where do you work?

A. I work for the FBI.

Q. What's your position with the FBI?

A. I'm a computer scientist.
Q. How long have you been a computer scientist with the FBI?
A. Approximately seven and a half years.
Q. Do you have any professional responsibilities in addition to being a computer scientist with the FBI?
A. Yes, I do.
Q. What are those?
A. I also teach.
Q. Where do you teach?
A. I teach at the School of Engineering at New York University.
Q. What do you teach?
A. I teach digital forensics.
Q. What's digital forensics?
A. Digital forensics is the concept of applying forensic science principles to investigating digital evidence.
Q. How long have you been an adjunct professor?
A. About a year.
Q. I'd like to talk about your education for a second. Do you have any undergraduate degrees?
A. Yes, I do.
Q. What was your undergraduate degree in?
A. It was a bachelor of science in computer science.
Q. How about graduate degrees?
A. I have a master of science in computer forensics, and a

master of science in computer science.
Q. You mentioned computer forensics. What's that?
A. It's another word for digital forensics. It is the concept of applying forensic science to investigating digital evidence.
Q. Prior to your work as a FBI computer scientist, do you have any other experience in the information technology industry?
A. Yes, I do.
Q. Could you summarize that for us, please.
A. Before I worked for the FBI, I worked for a litigation company as a digital forensics analyst.
Q. How long did you do that for?
A. About two years.
Q. When did you become an FBI forensic scientist -- excuse me -- computer scientist?
A. I was hired in September of 2012.
Q. Generally speaking, what are your responsibilities as a FBI computer scientist?
A. So, I work on a squad that investigates cyber intrusions. And my job is to work with the agents and analysts on that squad and provide subject matter expertise and perform technical analysis when needed.
Q. When you say cyber intrusions, what does that mean?
A. It's a fancy way of saying hacking.
Q. You mentioned some technical work that you do.
A. Yes.

Q. Can you tell us what you mean.
A. So, it is a wide range of tasks. Forensic analysis of computers, analyzing captured memory, reviewing log files, reverse engineering malware, also consult with agents prior to them interviewing witnesses, sitting in on interviews, things like that.
Q. Sir, are you familiar with the FBI CAT team?
A. Yes.
Q. C-A-T. What does CAT stand for?
A. That's the Cyber Action Team.
Q. What does the CAT team do?
A. The CAT team is managed out of our cyber division at headquarters. It is the FBI's incident response team for cyber incidents.
Q. When you say incident response team, what do you mean by that?
A. Incident response is the process of responding to an incident. So if an intrusion, a computer intrusion were to occur at a institution, and they reached out and called the FBI, depending on the scale of that intrusion, they might deploy the CAT team to that incident.
Q. How are you familiar with the CAT team?
A. I'm a member of the team.
Q. How do you become a member of the CAT team?
A. There is a three-part application process.

Q. Could you generally describe it.
A. The first part is a written application where you document your experience and education in the field. If you -- they accept your application, the next part is a practical. So it's approximately four days where they give you evidence, they give you limited information about a scenario. And you have to then analyze that evidence, and determine what happened.

The third part of the process, if you pass the second part, is a presentation. You then give a presentation -- almost like a mock presentation where you're presenting to both people that are technical and non-technical, and you have to explain what happened during this incident.

Q. Could you tell us what kind of investigations you've participated in as a member of the CAT team?
A. A wide range of computer intrusions, hacking intrusions, both nation state and criminal hacking.
Q. Just remind us, what is a nation state?
A. Nation state refers to hacking on behalf of either directly from or on behalf of a foreign government.
Q. Have you participated in trainings related to your work?
A. Yes, I have.
Q. What kinds of training have you taken?
A. I've taken numerous trainings related to forensics and other fields with information security.
Q. Have you received any kinds of certifications?

A. Yes, I have.
Q. What certifications do you hold?
A. Directly relating to forensics, I hold the GIAC, which is an organization, the certified forensic examiner as well as the certified forensic analyst, as well as several other certifications not directly related to forensics, but related to information security.
Q. Generally speaking, what kind of certifications are the information security certifications?
A. Certifications regarding just general information security, network traffic analysis, security in regards to special systems such as industrial control systems, things like that.
Q. In addition to the class you mentioned, have you ever done any other kind of presentations?
A. Yes, I've done internal trainings at the FBI.
Q. Anything outside the FBI?
A. Just the teaching I believe.
MR. KAMARAJU: The government would offer Mr. Berger as a expert in forensic computing, digital forensics, and computer science.
THE COURT: Any objection?
MR. BRANDEN: May I ask a couple questions?
THE COURT: Yes, you may.
BY MR. BRANDEN:
Q. Mr. Berger, have you ever testified in court before?

A. No, I have not.

Q. So you've never been approved as an expert before in the field that you're purporting to be an expert in today?

A. Not in court, no.

MR. BRANDEN: I have no objection, Judge.

THE COURT: Okay. He's recognized as an expert.

MR. KAMARAJU: Thank you, your Honor.

Before we proceed, we have a stipulation that we'd like to read into the record.

THE COURT: Yes, please.

MR. KAMARAJU: Ms. Hurst, can you pull up for just the parties and the Court and the witness Government Exhibit 3002, and just flip to the last page.

Paragraph 6 of the stipulation reads: It is further stipulated and agreed that this stipulation, as Government Exhibit 3002, and Government Exhibits 13501 through 1305-10 --

MR. BRANDEN: I think you said that incorrectly.

MR. KAMARAJU: Thank you.

1305-1, through 1305-10, Government Exhibit 1306-1, Government Exhibit 1301-1 through 1301-4B, Government Exhibit 1302-1, and Government Exhibits 1304-1 through 1304-3, may be received in evidence as Government Exhibits at trial.

And your Honor, we would offer the stipulation into evidence as well as all the exhibits referred to there.

THE COURT: Any objection?

MR. BRANDEN: No.

THE COURT: 3002 and all the exhibits referred to are received in evidence.

(Government's Exhibit 3002, 1305-1 through 1305-10 received in evidence)

(Government's Exhibit 1306-1, 1301-1 through 1301-4B, 1302-1 received in evidence)

(Government's Exhibit 1304-1 through 1304-3 received in evidence)

MR. KAMARAJU: If we can now publish the stipulation for the jury. If we can go to the first page. At the moment I'm just going to read the first two paragraphs.

If called as a witness, a representative of Google, Inc. (Google) with knowledge of the matter would testify that Government Exhibits 1305-1 through 1305-10 are true and correct copies of documents from the account joshschulte1@gmail.com, including subscriber information, e-mails, and Google searches conducted and websites visited by the user of that account, and the date and times those searches occurred and the websites visited search history, were made at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the regular practice of that business activity to maintain the records.

2. If called as a witness, a representative of Amazon.Com, Inc. (Amazon) with knowledge of the matter would testify that Government Exhibit 1306-1 contains true and correct copies of documents from Amazon associated with Amazon user account joshschulte1@gmail.com, which were made at or near the time by, or from information transmitted by, a person with knowledge of the matters set forth in the records; they were kept in the course of a regularly conducted business activity; and it was the regular practice of that business activity to maintain the records.

Now can we show for just the parties, the Court, and the witness Government Exhibit 1704.

Q. Mr. Berger, can you take a look at what's on the screen.

A. Okay.

Q. Do you recognize it?

A. Yes, I do.

Q. How do you recognize it?

A. There's slides I've prepared.

Q. Were they prepared in connection with your testimony today?

A. Yes, they were.

Q. They represent a summary of your testimony today?

A. Yes, they do.

Q. Do they summarize exhibits you reviewed?

A. Yes.

Q. Will it aid in your testimony today, Government Exhibit

1704?

A. Yes, it will.

MR. KAMARAJU: Your Honor, the government would offer Government Exhibit 1704 as a demonstrative.

MR. BRANDEN: No objection.

THE COURT: It's received in evidence.

(Government's Exhibit 1704 received in evidence)

MR. KAMARAJU: If we can pull that up for the jurors, please.

Q. Did there come a time when you became involved in an investigation into something called Vault 7?

A. Yes.

Q. When did you start working on the Vault 7 investigation?

A. That was approximately the middle of March, 2017.

Q. Were you present in court for the testimony of Jeremy Weber?

A. Yes, I was.

Q. Were you present for the testimony of Anthony Leonis?

A. Yes, I was.

Q. Did you hear them testify about the defendant's administrative privileges with respect to a EDG project called OSB libraries?

A. Yes, I did.

Q. Were you asked to review any forensic evidence relating to changes in the defendant's administrative privileges in OSB

libraries?
A. Yes, I was.
Q. Does this section of your presentation deal with that analysis?
A. Yes.
Q. Go to the next slide, please.
So Mr. Berger, it is a little blurry. Can you explain what we are looking at here?
A. So what we're looking at here is a query or a search done on a restored version of the database. This particular database was the Stash database that was saved on 4/16/2016. I was able to restore that database into an active database, and then search the data.
Q. If we can, what were you searching data for?
A. So this search was looking for activity between April 4, 2016, and the end of the database, so April 16. And it was specifically looking for activity referencing the user Schuljo.
MR. KAMARAJU: So can we just focus on the top two rows if we can blow those up, Ms. Hurst. Thanks.
Q. Could you explain what activity is reflected here.
A. Sure. So this is the -- the activity reflected here is the user Weber removing administrative access from the user Schuljo on the project OSB libraries.
Q. What's the date and time of that action?
A. That's April 4, 2016, at 11:21 a.m.

Q. If we can go to the next slide. Do you recall Government Exhibit 1061?
A. Yes.
Q. Who sent this e-mail?
A. This e-mail was sent from Josh Schulte.
Q. What is the date and time he sent it?
A. This was sent on April 14, 2016, at 3:39 p.m.
Q. If we go to the next slide. Do you see in this e-mail where the defendant asked to be allowed to administer OSB libraries?
A. Yes.
Q. In particular, do you see where he says, "I'd like to stay on along with Frank Stedman and Jeremy Weber as helping administrating them"?
A. Yes.
Q. Could you read the last line.
A. "So, if OSB and RDB would be okay with this, I would like to continue my active role with the libraries."
Q. Can we take a look at the next slide, please. What's this?
A. This is an e-mail that was sent from Anthony Leonis.
Q. Who is it sent to?
A. Sent to Josh Schulte, Jeremy Weber, JoJo, Frank, and Matthew. And it was cc'd to Sean, Richard, Frank Stedman, and Kevin.
Q. When was this e-mail sent?

A. This was sent on April 14, 2016 at 3:59 p.m.
Q. Do you recall Mr. Leonis testifying about this e-mail?
A. Yes, I do.
Q. Can we go to the next slide, please. Did Mr. Leonis authorize the defendant at that time to act as an administrator for OSB libraries?
A. No.
Q. Can we go to the next slide, please. We've looked at this before; is that right?
A. Yes.
Q. Can we focus on the last two entries. What are we looking at here?
A. So this represents the user Schuljo taking action to reinstate admin privileges on the project OSB libraries for the user Schuljo.
Q. When did he do that?
A. That was on April 14, 2016, at 4:05 p.m.
Q. When did this happen in relation to the e-mail from Mr. Leonis that we just saw?
A. It was about six minutes after.
Q. So let's go to the next slide and just recap.

Can you just walk us through the timeline here.

A. Sure. So the timeline references how on April 4, Mr. Weber removed the defendant's privileges to the OSB libraries, the admin privileges to the OSB libraries. On April 14, at 3:39,

the defendant requested his admin privileges be reinstated. 3:59 p.m., an e-mail response was sent saying the admin privileges would not be reinstated. And at 4:05 p.m. the defendant reinstated his own admin privileges.

Q. In addition to Mr. Leonis and Mr. Weber, were you also present during David's testimony?

A. Yes.

Q. Did you hear all three of them testify about certain actions on DevLAN on April 16, 2016?

A. Yes.

Q. What's your understanding of what those actions were?

A. My understanding is there were actions taken to lock down or harden the system.

Q. Were you asked to review any forensic evidence in connection with those actions?

A. Yes, I was.

Q. Can we go to the next slide, please. Could you explain what we're looking at here?

A. So these are two different search results on the same search, on the data from two different backups. So the first screenshot is from the Crowd database from April 15, 2016. The second screenshot is from the Crowd database on April 17, 2016. So, before and after April 16.

Q. What's reflected here?

A. So this was a search for -- to reflect all the group

memberships that user Schuljo was a member of.
Q. How do they change between April 15, 2016 and April 17, 2016?
A. On April 15, the user account was a member of the Atlassian administrators group. By April 17, he was no longer a member of that group.
Q. Can we go to the next slide. Was the defendant's privileges the only ones that were changed on April 16, 2016?
A. No.
Q. What's reflected on this slide?
A. So this is similar in that the first screenshot reflects the -- the Crowd database from April 15. And the second from April 17. The search on the first screenshot is reflective of all users that were member of a group with the word "administrator" in them. And the same for the second screenshot.
Q. How did it change?
A. So, there were several users that belonged to several different types of administrator groups on April 15. By April 17, there was only two accounts on the system that belonged to groups that had the word "administrator" in them.
Q. Sir, were you present -- excuse me. Sorry.
Was the defendant continued to be listed there?
A. No.
Q. How about Jeremy Weber?

A. No.
Q. How about Frank Stedman?
A. No.
Q. Sir, were you present for the testimony of Patrick Leedom?
A. Yes, I was.
Q. Did you hear Mr. Leedom testify about certain actions the defendant performed on DevLAN on April 20, 2016?
A. Yes.
Q. Generally speaking, what's your understanding of what the defendant did on that day?
A. My understanding is that on April 20, the defendant performed a snapshot reversion on the OSB ESXi server reverting the Confluence VM to a point in time when he was still part of the administrator group.
Q. Did you hear Mr. Leedom testify about what happened during that reversion?
A. Yes.
Q. What's your understanding of what happened?
A. In terms of?
Q. If any actions were taken.
A. There was activity shown on the system, there were -- evidence of log files being deleted. There is other activity that was being presented -- that was happening during that time frame coming from the defendant's DevLAN workstation.
Q. Did you hear Mr. Leedom testify about a March 3, 2016

backup file?
A. Yes.
Q. What's your understanding of the significance of that file?
A. That the March 3 backup -- Mr. Leedom testified that the March 3 backup file in his opinion was taken during that time.
Q. Were you asked to conduct any analysis of the EDG information disclosed by WikiLeaks?
A. Yes, I was.
Q. Have you formed any opinions with respect to that information?
A. Yes, I have.
Q. What opinions have you formed?
A. I was asked to perform analysis and conduct a timing analysis and look at the data that was on WikiLeaks.

My opinion of that analysis is that the data that was released on WikiLeaks came from a date range between March 2 and March 3, 2016.
Q. Was there a backup in existence on the Confluence -- was there a Confluence backup file in existence on DevLAN within that time range?
A. Yes.
Q. Which one was that?
A. It was the March 3 backup.
Q. So, if we go to the next slide and move on to the next one after that. I'd like to start with how you arrived at that

opinion. Could you describe your methodology, please.
A. Sure. So, I was asked to look at the data that was on WikiLeaks and determine when it came from in the Confluence system. In order to do that, we looked at the concept of version control, which both Stash and Confluence employ. Version control is a basic ability where you can make up dates to documents or source code. And when you save them, they don't completely overwrite your previous versions. The system keeps track of the history of versions so it goes from version 1, version 2.
Q. Could you just get a little closer to the mic?
A. Sorry.
THE COURT: And slow down, too.
THE WITNESS: Sorry.
Q. I'm sorry to interrupt.
A. That's okay. Because we knew that the version control existed on those systems, we could look at activity that happened on those systems and we could look at data that was posted on WikiLeaks.
We then looked for examples of data points of data that was saved in the system that was present on WikiLeaks. And data that was saved in the system that was not present on WikiLeaks.
Q. You mentioned version control. Could you explain what you're talking about there.

A. Sure. So the easiest way would be if you create a Microsoft Word document on your computer and you save it, you then open it, you want to make some changes to it. Instead of saving over the original file, you might go to file save as and save it as version 2. You make some changes later on, you go to save as version 3. You could then go into the folder on your computer and would you see three different versions of the document that reflect how it was when you saved it at each of those points in time.

MR. KAMARAJU: Can we go to the next slide.

Q. Did you analyze the Stash data that was released by WikiLeaks?

A. Yes.

Q. Could you walk us through how version control worked with respect to Stash.

A. So Stash employed a version control that's common in the software development industry. Underneath Stash it runs what's called GIT. The concept of GIT is when you update your software, and you write some code and you want to save it into the repository, you end up with what's called a commit. You are committing your code into the system. The code is saved, and a record of the date and time that you saved the code.

Q. So, let's walk through what you did. What was the first step for your Stash analysis?

A. We looked at the data that was on WikiLeaks and we tried to

identify documents that we would be able to identify commit actions on within the database.

MR. KAMARAJU: Can we go to the next slide, please.

Q. Are you familiar with a file called marble.horig?

A. Horig.

Q. Did you find such a file in the WikiLeaks release?

A. Yes, I did.

Q. Why did you look at that file?

A. So that file was a source code file. What I mean by that is source code is generally referred to as plain text. There are other types of documents, like Word documents and PDFs that have text and other information stored within them. We were aware that some of the documents that were posted on WikiLeaks were converted when they posted it. So, in other words, there might have been a Microsoft Word document for a user manual. WikiLeaks converted the document to PDF and posted that PDF. Because of that conversion, we couldn't make an identical match. With a plain text file, we found they had posted actual source code files without -- or what appeared had not actually been converted. They just took the file as is and posted it.

Q. What did you do with this marble file?

A. So we computed what's known as a hash.

Q. What's a hash?

A. So a hash is a way of taking data and generating a fingerprint for that data. The way a hashing algorithm works

is you feed data in or what's known as the input, and you get an output. The output looks like that string that's on the screen. Lots of letters and numbers.

The concept of hashing is that if you -- one of the concepts -- if you always feed in the exact same input data, you will always get the same hashing data. It's very useful in forensics if you want to confirm that two files are identical. If they look similar, you can then compute a hash on them, and then you'll see that the hash matches, and you would know these files are identical.

Q. Can we go to the next slide, please. Could you tell us what we're looking at here.

A. So this is some data that we retrieved from the Stash backup files. We looked at that particular file, marble.horig, and we were able to see what's known as the commit history for it.

Q. And there are a couple of things in the MD5 column that are highlighted in blue here. Do you see that?

A. Yes.

Q. Why are they highlighted in blue?

A. Those indicate that they matched the hash computed from the file as it appeared on WikiLeaks.

Q. Do you have an understanding of why there are two?

A. Yes. So, one possibility for it would be if someone saved a commit on February 26 at 9:36 a.m., they then made a change

one minute later at 9:37 a.m. It's possible that on March 1st, they realized that they didn't want that change anymore or maybe it was an inadvertent change and saved. They could have rolled back to the data that was on February 26 at 9:36 and recommitted that version.

Q. Can we look at the next slide, please. So, what are we looking at on this timeline?

A. This is just another representation showing that the files that we just looked at, and representing them across a timeline. The data points that are beneath the timeline that are in green, those are versions of the file that appeared on WikiLeaks.

Q. Let's take a look at another file. Next slide, please. What are we looking at here?

A. So, this another file that we identified referred to as solution events or the file name was SolutionEvents.cs. As the file appeared on WikiLeaks, we computed the hash value to be what you see on the screen.

Q. Is this another source code?

A. That's another source code file or plain text.

Q. Can we move to the next slide. Could you explain what's going on here?

A. Sure. So, similarly, we looked at the commit history for this particular file as well. And we noticed that on February 13, 2016, at 3:13 p.m., the file was committed and it

was identical to the file as it appeared on WikiLeaks.
Q. Based on your analysis of the marble and solution events file data, were you able to reach any conclusions?
A. Yes, I was.
Q. Can we go to the next slide, please. What conclusions were those?
A. So looking at the data that was both present in the database and present on WikiLeaks, and present in the database and not present on the WikiLeaks, we were able to determine at what point the data sort of stopped that WikiLeaks had.
Q. Let's take a look at the next slide. Is that represented here?
A. Yes, it is.
Q. So what was your conclusion as to when the data, the range for the data?
A. For Stash we identified the range of data being from February 26, 2016, at 9:36 a.m., and March 4, 2016, at 9:45 a.m.
Q. Can you remind us, was there an identical hash for the marble file at March 1st?
A. Yes, there was.
Q. Was there a reason why you didn't use March 1st here instead of February 26?
A. Yes.
Q. What's that?

A. The reason is because that the files were identical, we didn't want to assume that the data had to have come after March 1st. We took a more conservative approach and we slid our date back to being as possibly coming from after February 26 instead.

Q. We can move on to the next slide. Did you do a similar analysis with respect to Confluence?

A. Yes.

Q. Take a look at the next one. What are we looking at on this page?

A. So this is again another database search. What we're looking at here is a Confluence database backup from April 25, 2016, and we're looking at a list of revisions for a particular page.

Q. Okay. So let's just walk through this a little bit.

A. Sure.

Q. Let's start with the left the title content ID. What's that column?

A. So every page, even every page revision in Confluence gets its own unique content ID.

Q. And content type?

A. In this case they're all pages. There are other types of content, such as if you make an attachment to a page, that would be listed as its own unique entry in the database, and it would be of type attachment.

Q. And moving one more column to the right. What do we have there?
A. So that is the title. The left and the title 16 were just formatting, so the entire title would display in the window here. That is the title of this particular page.
Q. And moving over to version. What's listed in version?
A. So that's the version of the page. So, as you would update the page and new versions were created, it would keep track of all the previous versions.
Q. How many versions are reflected here?
A. So this query lists 17 versions.
Q. Moving over to the next column. Creation date. What's that?
A. So the creation date, as you can see is identical across all versions. It seems to have stored the creation date of the overall page, not each individual version of the page.
Q. Is there a column that shows when each version of the page was created?
A. Yes. The last mod date, the next column.
Q. And what's the column, prev ver?
A. That's a unique value that's assigned within the database for all the different versions of the same page.
Q. And page ID?
A. Not sure what the values that are null, what those reference. There are other types of content in the database.

Actually, I believe the page ID might reference for when there's content that's not pages, how it links back to a particular page.

Q. Can we go to the next slide, please. What's this?

A. This is a copy of one of the pages as it appeared on WikiLeaks.

Q. Which page are we looking at?

A. So it's identified here as saying user number 3375130's home. We identified this as being a version of the Michael R's home page.

Q. How did you do that?

A. So we looked at the page. We looked at the content on the page. We also looked what you're asking about in the previous slide, that prev ver number that was a unique value across all the different pages. You can see here that's actually part of the name of the page as it was pushed out on WikiLeaks. It says page_3375129.html.

Q. We just go back to the last slide. Can you point out where that number appears.

A. Sure.

MR. KAMARAJU: Go forward again.

Q. Are you able to tell by looking at this page what version of the page we're looking at?

A. Yes, so if you look at the bottom, you'll see how there are included links to previous versions. And the numbers one

through 16 are displayed. That indicated that this is the 17th version of the page.

Q. Can we move on to the next slide, please. How many versions of Michael R's home page are reflected here?

A. 17 versions listed.

Q. So, are we looking at the same number that existed on the WikiLeaks page?

A. Yes.

Q. Can we have the next slide, please. What's this?

A. This is another page that came from the WikiLeaks release.

Q. What's the name of this page?

A. It's entitled Build Felix LP.

Q. How do you know that?

A. It's the appears in the title bar of the browser right before it says Mozilla Firefox.

Q. You testified previously about a prev ver number; is that right.

A. Yes.

Q. Is there a prev ver number for this one too?

A. There is a number that's reflected in the file name here where it says page_52625416.html.

Q. Are you able to tell from looking at this page how many versions of Build Felix LP this is?

A. So this page lists that there are seven previous versions, indicating that this is the eighth version of the page.

Q. Can we go on to the next slide. What are we looking at here?

A. This is a query from the Confluence backup from April 25, 2016. Looking for all the pages that match that same prev ver, the 52625416.

Q. Can you tell from this when the eighth version of the Build Felix LP page was created?

A. Yes.

Q. When was that?

A. So I'm going to circle it right here. That was on March 2, 2016, at 8:01 a.m.

Q. I think you circled it there, too. When was the ninth version created?

A. It's in the same circle. The ninth version was March 3, 2016, at 6:47 a.m.

Q. And the information that WikiLeaks disclosed, was that from the eighth version or the ninth version?

A. That was from the eighth version.

MR. KAMARAJU: Can we move on to the next slide.

Q. So let's walk through this. What are we looking at here? Let's start on the left.

A. So this illustrates how on March 2, 2016, at 8:01 a.m., Build Felix version 8 was saved in Confluence. And the page in WikiLeaks shows seven previous versions.

Q. What do we know about the Michael R. home page version?

A. So on March 2, 2016, at 3:58 p.m., Michael R's home version 17 was saved in Confluence. And the Michael R's home on WikiLeaks shows 16 previous versions.

MR. KAMARAJU: Can we move on to the next slide.

Q. There a lot going on in this one. Let's take it slow. Start on the one on the left. So what are we looking at there?

A. Starting again from the left, from the top left.

Q. Yes. The March 2, 2016, 8:01.

A. March 2, 2016, 8:01 a.m. Build Felix version 8 was saved in Confluence, and the Build Felix page in WikiLeaks shows seven previous version.

On March 2, 2016 at 3:58 p.m. Michael R's home page version 17 was saved in the Confluence database, and the Michael R's home on WikiLeaks shows 16 previous versions.

On March 3, 2016, at 6:47 p.m. Build Felix version 9 was saved in Confluence. This version is not reflected in the data on WikiLeaks.

Q. Why is that significant?

A. It gives us an indication of where the boundary is of the data that WikiLeaks does not have.

Q. So what conclusions were you able to draw?

A. That the data that WikiLeaks had was between those two points.

Q. Let's move on to the next. What does this reflect?

A. This reflects both the Stash and Confluence analysis.

Looking at Stash, we can see that the data that was on WikiLeaks corresponds to the data from between February 26, at 9:36 a.m. and March 4, at 9:45 a.m.

Looking at the Confluence data points, we're able to get a smaller window that shows between March 2, 3:58 p.m. and March 3, at 6:47 a.m.

Q. So the band in blue there, what's that mean?

A. That is the band for the Confluence data points.

Q. Remind us, what are the end points for that?

A. March 2nd at 3:58 a.m. and March 3 at 6:47 a.m.

Q. Can we take a look at the next slide. Do you recognize what we're looking at here?

A. Yes, I do.

Q. What is it?

A. These are directory listings of Confluence backup files.

Q. Do you remember Mr. Leedom testifying about these?

A. Yes.

Q. I'd like to go to the next slide. Do you see any backup files that fit the criteria that you addressed earlier?

A. Yes, I do.

Q. Which one is that?

A. That is the Confluence backup file from March 3.

Q. Why does it fit your criteria?

A. That file was created on March 3, at 6:25 a.m. and finished completion at 6:29 a.m. That backup file, when it was

generated, fits within that window.
Q. You said 6:25 a.m. Do you see the date modified column?
A. Yes.
Q. What's the date modified column listed there?
A. 6:29 a.m.
Q. What's the difference?
A. That's just an indication of when the backup process first started creating the backup, and when it was finished writing the data to the file.
Q. And with respect to the tgz files, do you see any of those that match your criteria?
A. Yes.
Q. Which one is that?
A. The March 3 file.
Q. When was that created?
A. That was created, it looks from the name of the file, it was created initially at 6:25 and then finished saving at 6:29 a.m.
Q. Can we move to the next slide, please.
So, putting all this data together, what are we looking at here?
A. So this reflects the timeline, the combined timeline from the Stash and Confluence analysis. And it reflects how the March 3 backup file fits into that window.
Q. Does it fit into the window you had previously identified

with the blue band?
A. Yes.
Q. Let's move to the next slide, please. We just looked at this. What's the date accessed for the March 3 backup file?
A. The date accessed for the March 3 SQL file is 5:42 p.m. on April 20.
Q. What year?
A. Of 2016.
Q. How about that tgz file?
A. The date accessed for March 3 tgz file was April 20, 2016, at 5:43 p.m.
Q. We can go to the next slide. In addition to the work that you did on DevLAN, did you take at any of the defendant's home media?
A. Yes, I did.
Q. Could you describe generally how he had his home computer network set up?
A. Sure. So he had a desktop computer that consisted of four hard drives. There was a single hard drive that operated as the system drive, or in Windows referred to it as the C drive, and there were three additional hard drives that combined to form what's known as a RAID volume.
Q. What's a RAID volume?
A. So a RAID volume is a way of combining multiple hard drives and presenting to the user as a single large volume of data.

It has redundancy built in depending on the configuration, so if one those hard drives were to fail, you don't lose the data, the data is still stored on the other two, and you can replace that hard drive.

Q. Did you call it a RAID 5?

A. Yes.

Q. What's the five mean?

A. The RAID 5 is just a type of RAID configuration.

Q. You remember hearing earlier about virtual machines?

A. Yes.

Q. You remember hearing about how virtual machines can be created on computers?

A. Yes.

Q. Are you familiar with virtual machines?

A. Yes, I am.

Q. What are virtual machines?

A. Virtual machine is a way of representing a computer inside of a computer. It is a way that allows you to run different operating system other than the primary operating system you'd run on your main computer.

Q. Did the defendant run any virtual machines on his home computer network?

A. Yes.

Q. Let's take a look at the next slide. What are we looking at here?

A. So this is the initial power on screen to a Linux virtual machine that was present on the defendant's workstation.

Q. You see the bullets, dot dot dot dot dot?

A. Yes.

Q. What do those represent?

A. So when this virtual machine was powered on, it presented a prompt, you enter a password. This screenshot represents after you've typed that password, before you would hit the enter key, it represents a password being entered.

Q. So let's look at what happens next. Can we go to the next slide. What's this?

A. So after you have entered the correct boot password, the virtual machine would start to boot up. Once it finished that process, it would present you with the desktop and or a log on screen to get to the desktop.

Q. Do you see a user name here?

A. Yes.

Q. Whose user name is here?

A. Josh.

Q. What did you do next?

A. If you enter the password for that user account, and then click OK, you would be presented with the desktop for the virtual machine.

Q. Let's take a look at the next slide. What's this?

A. This is the desktop of the virtual machine.

Q. Just remind us, whose desktop?
A. This is the desk, the virtual machine that was on the defendant's computer.
Q. Do you see it says Linux Mint there?
A. Yes.
Q. Do you know what that is?
A. So Linux Mint is a particular distribution of Linux.
Q. When you say distribution, I just -- what do you mean by that?
A. So Linux itself is open source. The core part of the operating system, different people, different organizations will take that and package it in different ways, customize how it looks with different utilities and they'll release different distributions of Linux.
Q. On the left side there, starting with computer. What are those icons?
A. Those are desktop icons.
Q. Are those icons the way it appears on the defendant's virtual machine desktop?
A. Yes.
Q. Let's walk through. The green folder marked "home," what's that?
A. That's the home folder for the user account that we're logged into here. The home folder is similar to how your home folder works on a Windows or Apple computer. Within there you

might have folders for documents, pictures, videos, things like that. It's where you put most of your user content for yourself. Different -- each user account would have their own home folder.

Q. The one below that, what's that?

A. That's an icon for the Tor browser.

Q. What does that icon represent?

A. So the Tor browser is a web browser that allows you to connect to the Tor network.

Q. What's the Tor network?

A. The Tor network is a system of computers that are connected, if you connect to it through a Tor browser, it allows you to connect to websites in a way that those websites are not able to trace where you're coming from.

Q. How does that work?

A. It essentially routes your traffic through a series of encrypted tunnels through a series of different computers that are running Tor software.

Q. When you're using Tor, are you able to see any different websites?

A. Yes, you are.

Q. Could you explain that, please?

A. You're able to see what's referred to as a Tor hidden service. That is a web server that is running specifically on the Tor network. Whereas most websites you go to might end in

dot com or dot net, a Tor hidden service would end in the dot onion phrase. The unique feature of the Tor hidden service, just as you are using the Tor browser, you're protecting where no one can see where you're coming from. A Tor hidden service is hiding where it's being hosted. So if an organization wanted to set up a web server, and allow people to connect to it but make it very difficult to determine its location, they could run it as a Tor hidden service.

Q. Could you give us an example of a Tor hidden service?

A. I believe WikiLeaks has a link to a version of their site. It ends at dot Onion.

Q. What's the icon below the Tor browser there?

A. That's for VeraCrypt.

Q. What's that?

A. VeraCrypt is an encryption program, it's used to encrypt and decrypt data.

Q. What's encryption?

A. Encryption is a way of securing your data. Obfuscating it so if you use a particular key or password to lock that data, you're unable to get back in and see that data unless you have the correct password.

Q. Generally speaking, how does VeraCrypt work?

A. So, there's two methods that are generally used. You can either encrypt a hard drive completely, or you can create what's known as an encrypted container. This would -- think of

it as kind of like a zipped file, where it is a file where you put other files. You create an encrypted container, you would mount it and it appear as a window. You can then drag other files into it. When you unmount that encrypted container, it would go back to being a single file on your computer that is encrypted. In order to then mount that file again and view its contents, you would need the password or key for that file.

Q. Did you try to mount any encrypted containers?

A. Yes, I did.

Q. Let's walk through that process. Go to the next slide. What are we looking at here?

A. So this a screenshot of when you open VeraCrypt, as indicated here, I've selected a particular file here.

Q. That says slash home. What's that a reference to?

A. So on Linux, the slash home is where the user account folders would go. So, under the slash home directory, you would see a slash Josh directory. That would be indicative of the home folder for the user account Josh.

Q. What's this file called?

A. This file is called data.bkp.

Q. Let's go to the next slide. What happens after you try to mount it?

A. So when you click mount, you would be prompted to enter the password for that container.

Q. Did you try to enter the password?

A. Yes, that's represented by those black circles in the password box.
Q. What happens after you enter the password?
A. After that, you would then click OK.
Q. Okay. Once you click OK, what happens?
A. Another prompt would come up, prompting for an administrator password.
Q. What's an administrator password?
A. So, Linux, the administrator account is referred to as the root account. This is prompting you for the administrator password or the password of a user who has privileges to mount. The reason being is that mounting, when you're -- when you're decrypting an encrypted container, it's what's known as mounting a file system. It's going to appear as a virtual disc. That's how VeraCrypt connects the data to the system. Mounting a file system in Linux requires root privileges.
Q. Do you know if the defendant ever tried to mount any encrypted containers?
A. Yes.
Q. I'd like to direct your attention to April 18, 2016. Do you know if he tried to mount any containers on that day?
A. Yes.
Q. Let's go to the next slide. How do you know?
A. You can see here, these are entries from a particular log file referred to as auth.log.1. On April 18, you can see here

particularly the entry.

Q. Let me ask you a question before you go on. What's auth. log?

A. So the auth. log represents a log file on Linux where authentication related activity is stored.

Q. What do you mean by authentication?

A. It would be like logging in with your password.

Q. So, now I believe you were about to talk about some particular entries here.

A. Yes.

Q. Please describe those?

A. So you can see the two lines where I've circled the beginning of the line, towards the end of that line where it says command user bin VeraCrypt core service, then again on the next line. This was indicative of trying to mount an encrypted container with this particular version of VeraCrypt.

The reason that it says one incorrect password attempt, what I mentioned before where you need root privileges, when VeraCrypt tries to mount the container it doesn't have root privileges. It then prompts you for an administrator password, and will be able to mount the container given an appropriate password.

Q. How do you know that's how VeraCrypt works?

A. Because I researched the product, researched this particular message, and we recreated the steps of mounting it

and verifying the contents of the log file.
Q. Do you know if the defendant actually accessed the VeraCrypt container?
A. Yes.
Q. Go to the next slide, please. How do you know that?
A. So this file represents recently used activity. Several versions of Linux have this file, it's kind of like a history file for things you do on a file system. You can see here that it references the file/home/josh/data.bkp. You can see the application name referenced with that file was VeraCrypt.
Q. What's the date of this access attempt?
A. So the date on the access attempt, I'll circle it right here. It's listed here as April 19, 2016, at 3:03 a.m. However that is marked as Zulu time. So that would correspond with 11:03 p.m. on April 18.
Q. That would be local time?
A. Yes.
Q. This is from April 18. Were you asked to look at any other forensic evidence from April 2016 from the defendant's home network?
A. Yes.
Q. Let's start with April 23, 24. You know what Tails is?
A. Yes, I do.
Q. Go to the next slide. Do you know what a SATA adapter is?
A. Yes, I do.

Q. What are we looking at?
A. This is an order confirmation e-mail from Amazon sent to Josh Schulte.
Q. And what's the date of it?
A. Sunday, April 24, 2016, at 12:39 a.m.
Q. What's the product that's referred to here?
A. The product listed is an Inatek USB 3.0 SATA.
Q. You see the name am is cut off there a little bit.
A. Yes.
Q. Let's go to the next slide and see if we can expand that. What's this?
A. So these are the results of a search warrant to Amazon for those order details.
Q. Do you see an item description?
A. Yes.
Q. Could you read that description.
A. Sure. Inatek USB 3.0 to SATA dual bay USB 3.0 hard drive docking station with offline clone function for 2.5-inch and 3.5-inch HDD SSD SATA (SATA 1/2/3).
Q. Do you know what that is?
A. Yes.
Q. What is it?
A. So this is what's referred to as a docking station. It is a small device that you would be able to hook up to your computer and insert hard drives into it.

Q. Do you see where it says shipped?
A. Yes.
Q. What's the shipped date listed there?
A. The ship date is listed as April 24, 2016.
Q. Is that the same date as we saw the order confirmation for?
A. Yes.
Q. Do you know if Amazon offers same day shipping?
A. I've heard that they do, yes.
Q. Do you see the ship method listed as lasership_INJ_same?
A. Yes.
MR. KAMARAJU: Can we go to the next slide, please.
Q. What are we looking at here?
A. So these are the results of a search warrant to Google for searches from the defendant.
Q. Let's just start at the bottom one. What's the date and time of that?
A. That is April 24, 2016, at 2:42 p.m. UTC which would be 10:42 a.m. local time.
Q. Is that after the order confirmation that we looked at from before?
A. Yes.
Q. What did the defendant search for here?
A. He was searching for a SATA adapter.
Q. What's a SATA adapter?
A. A SATA adapter is something that allows you to connect a

SATA interface on a hard drive and connect it to another type of interface.

MR. KAMARAJU: Your Honor, may I approach?

THE COURT: Yes, you may.

Q. I'm showing what's been entered into evidence as Government Exhibit 1603, 1609, and 1610.

Do you recognize Government Exhibits 1609 and 1610?

A. Yes.

Q. What are they? You can take them out of the bag, too.

A. 1609 and 1610, right?

Q. Yes.

A. They are both hard drives.

Q. I believe we saw a stipulation before that they were -- I'll put the stipulation in.

Now hard drives, could you take them out of the bag, please.

A. Sure.

Q. Would that kind of hard drive work with the Inatek SATA adapter?

A. Yes.

Q. Could you demonstrate for jury how that would work.

A. Sure. So, if you see on the side right here there is some connections. These connections right here, there is a longer connection and a shorter connection. The shorter connection, longer connection are both the data channel and the power

channel. The SATA adapter that was ordered, if you can picture like a toaster with two slots on top of it. You would take the hard drive, and you would, with those connections facing down, drop it into one of the slots, it would meet receiving connections on the inside of the device.

Q. Once you connect to the device, what would you be able to do?

A. Once you connect to the hard drive into the device, the device would have a power cord, you plug and give it power and would have a USB cable coming out of it. You could then plug that into your computer and you could read and write data from the hard drive.

Q. Government Exhibit 1610.

A. Okay.

Q. Would that type of hard drive work with the SATA adapter?

A. Yes, it would.

Q. What's the size of Government Exhibit 1609 and Government Exhibit 1610?

A. Each one is a one terabyte hard drive.

Q. Let's take a look back at the Google searches for a second. Do you see a search on April 24, 2016, at 14:4:37 UTC?

A. Yes.

Q. Do you see where it says searched for SATA PCI card?

A. Yes.

Q. What's a SATA PCI card?

A. A SATA PCI card is another way of connecting a SATA hard drive to your computer. Whereas the docking station would allow you to connect hard drives externally outside your computer, a SATA PCI card would be a card you install inside your computer. Most desktop computers have what we refer to as expansion slots. These are empty slots that the manufacturer gives you to add functionality later on. You would open up the side panel of your computer and insert the PCI card. On the card itself there would be additional ports to connect to a SATA hard drive.

Q. Would that work the same way with respect to data transfer as the SATA adapter?

A. Yes.

Q. So would you be able to transfer data to the hard drive that you had connected?

A. Yes.

Q. Can we take a look at the next slide. What are we looking at here?

A. This is a shipping confirmation e-mail from Amazon.

Q. If we just blow up the top there. What's the date and time?

A. I believe that is Sunday, April 24, at 2:14 p.m.

Q. Do you see under where it says "Hello Josh Schulte"?

A. Yes.

Q. What's the product that was shipped?

A. The Inatek USB 3.0 SATA.
Q. All right. What does it say under "arriving"?
A. It say it's arriving Sunday, April 24.
Q. Of what year?
A. 2016.
Q. Let's take a look at the next slide, please. What are we looking at here?
A. So this is a file information for a particular file that was found on the defendant's computer.
Q. What's the file that was found?
A. The file itself is Tails-I386-2.2.1.torrent.
Q. We talked a little bit about Tails before. What is that?
A. So Tails is an operating system that allows you to connect directly to the Tor network. It's unique in that it -- one of its capabilities is it forces all of your traffic to go directly through the Tor network.
Q. How does it work?
A. So you would download the Tails file. You would then copy the data on to some kind of removable media, so maybe a DVD or a USB drive. You would then power off your computer and turn it back on, and you would indicate for your computer to boot from that device. Instead of loading the operating system like Windows that you would normally boot into, you would boot into an operating system running from this device.
Q. What's the impact of booting from the device rather than

from your regular operating system?
A. So by booting from this device, the entire operating system is loaded into memory. And everything about Tails is designed to operate inside of memory and not touch the hard drive.
Q. So, if you were using Tails, would there be signs on your hard drive of the activity you were doing?
A. No, there would not.
Q. Can you use Tails with a virtual machine?
A. You can create a virtual machine of Tails, yes.
Q. Are you, when you are in a virtual machine, are you able to bring data in from your regular computer?
A. Yes, you can.
Q. Are you familiar with the concept mounting?
A. Yes.
Q. What's mounting?
A. So mounting is in the Linux operating system, if you want to connect to data on another computer or a server you have to mount the data. So you connect to that particular share of data, and you assign the mount point on your system. It would just be an empty folder. Once you mount it, if you go into that folder, you would be looking at the data on the other system or the server.
Q. Can you tell when the Tails file was downloaded?
A. Yes.
Q. When is that?

A. April 24, 2016, at 5:02 p.m. local time.
Q. How do you know that's the date?
A. You can see here on the last written entry.
Q. Do you also see an entry for file created?
A. Yes, I do.
Q. What's listed there?
A. May 10, 2016 at 9:06 p.m.
Q. Is there a reason why the file created date is listed as May 10 versus April 24?
A. Yes.
Q. What's that?
A. This is generally what happens when you download a file, and you move the file from one piece of media to another piece of media. The way file systems metadata works, the last written or last modified date is generally preserved when you copy files from one system to another. However, the other attributes are generally recreated.

So if you have this file on a thumb drive, and you copy it over to the computer, the file on the computer would have a creation and a last accessed of the most recent time. However, the last modified or last written date would be preserved in that transfer.

Q. Did you see any evidence that the defendant had engaged in that kind of copying activity on his home network?
A. Yes.

Q. Could you explain, please.
A. So, the computer we looked at, particularly the C drive, had activity on it where there were files shown to have been last modified at a point prior in time to when there was indication that the drive was reformatted.
Q. Let's take a look, you have it in front of you at Government Exhibit 1603, a thumb drive recovered from the defendant's apartment.
A. Yes.
Q. You can take it out of the bag. You ever seen Government Exhibit 1603 before?
A. Yes.
Q. How do you recognize it?
A. I have my initials on the evidence item.
Q. Have you reviewed a forensic image of that thumb drive?
A. Yes, I have.
Q. Were there any programs on there?
A. Yes, there were.
Q. Which programs?
A. The program Eraser Portable.
Q. What's Eraser Portable?
A. So Eraser is a program that's designed to securely delete files. Eraser Portable is a slightly modified version of the program that allows it to run off of a piece of removable media without being installed on the computer.

Q. When you say "securely erase," what are you referring to?
A. So, the way a file is normally deleted would not be considered secure. The way files are stored on your system, you can think about it as a table of contents that points to where files are. Generally when you delete a file, the file is marked in the table of contents as being deleted. So the operating system no longer would show you that file, but the data for the file is still there and is able to be recovered with forensic software.

Securely deleting a file would go to the location on the hard drive where the content of that file is stored, and overwrite that data.
Q. Take a look at the next slide, please. What are we looking at here?
A. So this a screenshot from a forensic program showing the basic folder structure and some files from that thumb drive.
Q. Can you explain the folder structure.
A. So at the top here, we have this Eraser Portable directory. Within the Eraser Portable directory, there is an app directory, a data directory, and an other. Within the data directory there is a settings directory, that stores information about the program, certain configuration options, things related to its activity. Within the Eraser directory under the app directory, which is here, that's where the actual program itself resides.

Q. Do you see a file called schedlog.txt?
A. Yes, I do.
Q. What's that file?
A. So that is a log file that records, among other things, when Eraser Portable starts and stops.
Q. Did you look at the schedlog file?
A. Yes, I did.
Q. Let's go to the next slide, please. What's this?
A. This is the content of the schedlog file.
Q. Does it show that the Eraser Portable program was opened on the thumb drive in 2016?
A. Yes, it does.
Q. When was it first opened?
A. It was first opened on April 23, 2016, at 6:12 p.m.
Q. Was the program ever closed?
A. Yes, it was.
Q. When was it closed?
A. April 28, 2016, at 8:36 p.m.
Q. So, during that five-day period, was the Eraser Portable program running?
A. Yes.
Q. Have you looked at the program's activity during that period?
A. Yes.
Q. Can we look at the next slide, please. What are we looking

at here?
A. This is a screenshot from a forensic program showing the app directory. You can see here that there is a series of files, some of which are overwritten or partially overwritten, and their corresponding file date -- the date and time of those files.
Q. Which ones are the overwritten files?
A. So you can see here, the -- let me circle it. You see that little icon there. It's got a -- little hard to see here. A little red in the bottom-right hand of that icon. That indicates that it's deleted or overwritten.
Q. So, you see that entrance for default.ers?
A. Yes.
Q. What's that kind of file?
A. So the default.ers file is a file that's used with Eraser Portable. It keeps track of entries in the queue or jobs for Eraser to conduct.
Q. So as part of your analysis, did you examine the default file?
A. Yes, I did.
Q. Were there any particular properties of the file that you focused on?
A. Yes.
Q. What were those?
A. The size of the file.

Q. Why did you focus on size of the file?

A. So the file, the default.ers file, the file size is directly proportional to the entries that are entered into the Eraser program.

Q. To be clear, is there a relationship between the size of the file and the underlying file that the program is trying to delete?

A. Yes. So the files that you would add into Eraser, the files you were trying to delete, those pads to those files are stored in this file. So as you would put more files in, or have files that have longer pads, the default.ers file would grow.

(Continued on next page)

BY MR. KAMARAJU:

Q. And for purposes of the size of the default file, does it matter how big the actual file that you're trying to delete is?

A. No.

MR. KAMARAJU: Let's take a look at the next slide, please.

Q. What are we looking at here?

A. So, these are two different entries that were on the drive, listed under default.ers. They each have different files that were listed in that queue.

Q. Could you identify the files that were listed in the queue in the top selection?

A. So, on the top, we -- there is a -- there are two folders, Brutal Kangaroo and ArrayList. On the bottom, there are five files. They're data6.bkp, data5.bkp, data4.bkp, data3.bkp, and data2.bkp.

Q. From the file pack, can you tell what drive these documents are -- sorry, these files were on?

A. Yes. They were on the D drive.

Q. Now, you testified about the size of the default.ers file. Is there a relationship there between the file path size and the size of the file?

A. Yes.

Q. So when you type in, for example, Brutal Kangaroo versus ArrayList, will the file size be different?

A. Yes, it would.
Q. And have you heard testimony about Brutal Kangaroo before?
A. Yes.
Q. What's your understanding of what Brutal Kangaroo is?
A. My understanding is it is a project that was worked on at the CIA.
Q. And who worked on it at the CIA?
A. Josh Schulte.
Q. And the naming convention, data.bkp -- data 1, data 2, data 3, data 4 -- did you see that naming convention used anywhere else on the defendant's computer?
A. Yes.
Q. Where was that?
A. That would be in the container that he used for encrypted data within the search engine.
MR. KAMARAJU: Let's take a look at the next document.
Q. Can you tell us what we're looking at here?
A. This is a demonstration of how Eraser Portable looks. You can see when the program is open there is an area where you would add files. On this particular screenshot, the folder ArrayList is in that list.
MR. KAMARAJU: Let's look at the next one.
Q. What's reflected here?
A. So, this reflects both the ArrayList folder and the Brutal Kangaroo folder added.

Q. And on the left side of those file paths, where it says D colon --

A. Yes.

Q. -- what does that reflect?

A. That represents the -- the D represents the drive those files reside on, and then everything else is the folders and subfolders that they belong to.

MR. KAMARAJU: OK. Let's look at the next slide.

Q. What are we looking at here?

A. So, this represents those five BKP files being added into the Eraser program.

Q. Now, did you examine that the way the default ERS reacted when you were entering these steps?

A. Yes.

Q. Did that match the forensic evidence you saw in the Eraser Portable thumb drive?

A. Yes.

Q. Did you arrive at any conclusions about how the defendant used Eraser Portable between April 23 and April 28, 2016?

A. Yes.

MR. KAMARAJU: Let's take a look at those. Can we go to the next slide, please.

Q. Let's just start with April 23. What happened then?

A. On April 23, at 6:12 p.m., the defendant opens Eraser Portable.

Q. What happens next?
A. By 6:14, so two minutes later, the ArrayList item had been added to the queue for removal.
Q. And generally speaking, how did you arrive at that conclusion?
A. So, we looked at the activity in the over, partially overwritten and deleted files and their file sizes.
Q. What's the next thing that happened?
A. So, at April 23, by 6:20 p.m., both Brutal Kangaroo and ArrayList had been added to that queue.
Q. Now, do you see there's an entry, or there's a line there that's marked off in blue?
A. Yes.
Q. Now, the events that are marked off in blue, were you able to tell the order in which those events occurred?
A. No.
Q. Why is that?
A. It's just the nature of how the program works.
Q. So without referencing the order, what were the events that occurred during that time?
A. So, the two things that happened were the Eraser program was run on the Brutal Kangaroo and ArrayList folders; that means they were deleted. And the five BKP files were added to the queue.
Q. And were those files that were deleted using Eraser

Portable, the dot-BKP files?
A. No.
Q. How do you know that?
A. Because, again, the way the file operates and they were still in that ERS file when the program was closed out.
Q. And when was the program closed out?
A. On April 28, 2016, at 8:36 p.m.
Q. Does Eraser Portable securely delete all the files on a hard drive or just specific files?
A. Just the specific files you tell it to.
Q. Are there programs that securely wipe the entire hard drive?
A. Yes, there are.
Q. Did you find any forensic evidence of any of those types of programs on the defendant's home network?
A. Yes.
Q. What programs did you find?
A. The program is named Darik's Boot and Nuke, also referred to as DBAN.
MR. KAMARAJU: Can we go to the next slide.
Q. What are we looking at here?
A. So, this is from a forensic program looking at the file information before the file containing DBAN.
Q. When was DBAN downloaded?
A. DBAN was downloaded on April 30, 2016, at 11:28 a.m.

Q. Do you see the file-created date?
A. Yes.
Q. What's listed there?
A. May 5, 2016, at 9:59 p.m.
Q. Why is that date, May 5, if DBAN was downloaded on April 30?
A. Same as what we've, what I talked about earlier. If you move files from one drive to another, specifically one that maybe was reformatted, generally the last modified or last-written time is preserved across that transfer.
Q. Do you see the row there at the top that says file EXT and then it says ISO?
A. Yes.
Q. What's an ISO file?
A. So, ISO file is a type of file. It's generally used for the contents of disk images, such as DVDs, CDs or image for a USB thumb drive.
Q. What happens if you click on the ISO file?
A. Depends what software is installed on your computer. If you don't have the appropriate software, then you're not going to be able to view it on this.
Q. If you are successfully able to open an ISO file, what happens next?
A. You could view the contents that are contained within the file, or you could also view it in a program that would allow

you to write it to some kind of removal media, so a DVD or a thumb drive.

Q. Did you access this ISO file?

A. Yes, I did.

MR. KAMARAJU: Let's take a look at the next slide.

Q. What are we looking at here?

A. So, I took the ISO and booted it up in a virtual machine, and this is the screen that shows up when you power it up.

Q. Do you see the red "warning" label under Darik's Boot and Nuke?

A. Yes.

Q. Could you read that, please?

A. Sure. It says: "Warning. This software irrevocably destroys data."

Q. What's that mean?

A. That means that it would securely erase data where, in a way that you cannot recover the data.

Q. And do you see down below where it says, "Press the F2 key to learn about DBAN"?

A. Yes.

Q. Did you press the F2 key?

A. I did.

MR. KAMARAJU: Let's take a look.

Q. What's this?

A. So, this is a screen that displays more information about

the program.

Q. Could you read the first paragraph, please?

A. "Darik's Boot and Nuke (DBAN) is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction."

Q. Let's start at the top. What's a self-contained boot floppy?

A. Similar to how we described Tails earlier, you would take the contents, put it on some kind of removable media and you can boot off of it. It's a self-contained operating system. It does not require an operating system to have been present on the computer in order to utilize this.

Q. What does it mean to securely wipe a hard disk?

A. So, as I talked about earlier, wiping a hard disk securely is the same as wiping a file securely. It's the difference between deleting it and just marking it as deleted or going over every single possible space on the hard drive and overwriting it.

Usually when you securely wipe a hard drive, you overwrite it with either all zeros or all random data.

Q. On Government Exhibits 1609 and 1610, the hard drives we looked at before, did you see any data on those?

A. No, I did not.

Q. Could you read the next line?
A. "This program clears directly attached IDE, PATA, SATA, SCSI and SAS disks. Some USB and IEEE 1394 (Firewire) devices may be recognized. DBAN requires a computer with a PCI bus and 32 megabytes of memory."
Q. So the acronyms in the first sentence, the ones starting with IDE and going forward, what do those represent?
A. Those just refer to different types of hard drive interfaces.
Q. Do you see the one called SATA?
A. Yes.
Q. Have we heard that term before?
A. Yes, we have.
Q. OK. When?
A. When we were talking about the hard drives that are in front of me here.
MR. KAMARAJU: Let's take a look at the next slide.
Q. What's this?
A. So, this is another information screen that's present from the DBAN menu.
Q. And what information is it presenting?
A. It shows different options you can use to wipe hard drives.
Q. Now, were you able to also examine any of the log-in activity on the defendant's home network?
A. Yes.

MR. KAMARAJU: Let's go to the next slide, please.

Q. I'd like to focus on April 30 to May 1, 2016. OK?

A. OK.

Q. Were you able to look at data from those dates?

A. Yes.

Q. Now, is this the auth.log file again?

A. This is the auth.log file. I believe we were looking at the auth.log 1 file, which is just a rollover of the auth.log file when it gets to a certain size.

Q. Remind us what the auth.log file is.

A. The auth.log just stores authenticated events.

Q. Looking at this file, are you able to tell whether the defendant logged in to his virtual machine on April 30, 2016?

A. Yes.

Q. How do you know?

A. Just going to circle a line right here.

So, those lines that indicate cinnamon-screensaver-dialog gkr-pam unlocked login keyring, that's an indication that the screen saver for the virtual machine was unlocked with a password.

Q. Let's just walk through that. What is a cinnamon-screensaver?

A. Cinnamon refers to the graphical user interface that was present on the virtual machine.

Screen saver is -- was very common in older computers where

you had to worry about screen burn-in if you left your computer on the same data for a long period of time. So after a few minutes, the screen saver would kick in and just animate something to prevent screen burn-in. Now they're more common to prevent unauthorized access to a computer, so when you're away from your computer for a few minutes, it might lock and then require you to unlock it when you return to your computer.

MR. KAMARAJU: Let's turn to the next slide.

Q. What's this?

A. This is just more activity also contained in the auth.log.

Q. Specifically, were you able to tell if the defendant logged in to his VM on May 1, 2016?

A. Yes.

Q. And how do we know that?

A. Again, I'll circle it here.

There is additional entries displaying how the screen saver was unlocked during this time.

Q. So what times did the defendant log in to his virtual machine?

A. There's an entry on May 1 at 1:57 a.m. There's another entry later that morning, at 2:34 a.m. There's one at 2:56 a.m. and again at 3:18 a.m.

Q. Remember we talked a little about mounting data into your VM?

A. Yes.

Q. Between April 30 and May 1 of 2016, did the defendant mount any data into his VM?
A. Yes.
Q. What did he mount?
A. On May 1, he mounted a folder on his computer. Specifically, the D drive on his computer was connected into the virtual machine.
Q. And the data.bkp files we looked at before, were those saved in his D drive?
A. Yes.
MR. KAMARAJU: Let's take a look at the next slide.
Q. Did you look at any additional Google searches that the defendant did?
A. Yes.
Q. Did you look at searches that he did between the evening of April 30, 2016, and May 1, 2016?
A. Yes.
MR. KAMARAJU: Let's go to the next slide.
Q. What are these?
A. So, these are those additional Google searches, starting on May 1, 2016, at 2:51 a.m. UTC time.
Q. Let's start at the one all the way at the bottom. What's the date and time of that search?
A. The date and time is May 1, 2016, 2:51 a.m. UTC. So if we go back four hours, that's going to be on the evening of April

30, 2016, at 10:51 p.m.

Q. And what did the defendant search for?

A. He searched for Western Digital disk wipe utility.

Q. What's Western Digital?

A. It's a hard drive manufacturer.

Q. Government Exhibits 1609 and 1610, what's the manufacturer of those hard drives?

A. For 1610, it's a Western Digital drive. And for 1609, it's also a Western Digital drive.

Q. Now, what's a disk-wipe utility?

A. It's a utility similar to what we talked about with DBAN. It's a utility that allows you to wipe a drive.

Q. Let's move up a little bit. Do you see how that same search the search for Western Digital disk wipe utility, is repeated a few times?

A. Yes.

Q. Do you have an understanding as to why that is?

A. One possibility would have been if you searched for something in Google and you see the results, you visit those pages and then you go back to your search results. Sometimes when you go back, the looking at your results might trigger Google to record it as another search.

Q. Let's take a look at one of the different ones. Do you see an entry for May 1, 2016, at 02:55:27 UTC?

A. Yes.

Q. And remind us. What's that in local time?
A. That would on the evening of April 30, 2016, at 10:55 p.m. local time.
Q. What did the defendant search for there?
A. He searched for a Samsung SSD wipe utility.
Q. What's a Samsung SSD?
A. So, Samsung is another hard drive manufacturer. The SSD refers to a type of hard drive. Conventional hard drives, such as the two up here, have what's called platters in them. They are disks that spin at a high rate of speed, and there's an arm that goes across those drives and magnetically reads and writes data to them.

SSD is a solid state drive. There are no moving parts. Everything is stored on internal circuitry.

Q. What's a Samsung SSD?
A. That would be a utility to wipe a Samsung SSD drive.
Q. Did the defendant's home network include any Samsung SSDs?
A. Yes, it did.
Q. Where?
A. The C drive, or the primary drive of the workstation, was a Samsung SSD drive.

MR. KAMARAJU: Let's take a look at the next slide.

Q. What are we looking at here?
A. These are more Google searches.
Q. Let's start at the bottom. What's the date and time of the

bottom search?
A. 2016, May 1, 7:18 UTC, so that would be 3:18 a.m.
Q. And what's the search?
A. The search was "how long does it take to calculate MD5."
Q. What's MD5?
A. So, MD5 is a type of hash algorithm.
Q. Remind us. What is a hash algorithm?
A. It's used to generate a unique fingerprint of a file.
Q. What does it mean to calculate MD5?
A. So, in order to generate that MD5, there is a mathematical computation that has to take place. We talked about the MD5 algorithm. You feed data into it and the output is that value. Inside that algorithm, there is a lot of mathematical computation that's going on.
Q. And what gets spit out at the end of that?
A. A value that looks like a bunch of letters and numbers.
Q. How do you typically use that hash value?
A. So, you can use it in a couple different ways. In -- one way would be to look at two files that look very similar to each other, you want to know if they're identical.

Another way is if you're transferring data. If you're sending data from one person to another, you might hash the file before you send it, generate that fingerprint. You then send the file to another person. Once they've received the file, you could ask them to calculate the MD5, and then you can

see if they match. If they match, then you know the file was transferred successfully.

Q. Let's go two entries up. Do you the line that says 07:18:45 UTC?

A. Yes.

Q. And what's that in local time?

A. That's going to be 3:18 a.m.

Q. And what website was visited there?

A. He visited a site researchgate.net, and it was a post entitled "What Is the Fastest Way to Hash MD5 Large Files?"

Q. Is there any correlation between the calculation of an MD5 file and the size of the files you're trying to hash?

A. Yes.

Q. What is it?

A. So, because a hashing has to take into account the entirety of the file, as the file gets bigger, there's more computation that has to take place.

Q. Let's take a look at the next one up. What's the date and time there?

A. So, that's May 1, 2016, 7:21 UTC, so that's going to be 3:21 a.m.

Q. What website was visited there?

A. That website was superuser.com, and it looks like an article entitled "How Can I Verify That a 1TB File Transferred Correctly?"

Q. Do you understand what the reference to TB is?
A. Yeah, I understand that to refer to a terabyte.
Q. What's a terabyte?
A. It's a measure of data size.
Q. And how big is it?
A. It's fairly large.
Q. Is it -- could you compare it to megabytes, for example?
A. Sure. So, if you have -- I'm sorry.
If you have a megabyte of data, if you have a thousand megabytes, you would have what is known as a gigabyte. If you have a thousand gigabytes, you would have a terabyte.
Q. Now, during the time of -- withdrawn.
Did you hear Mr. Leedom testify about the size of the Confluence and Stash backups?
A. Yes.
Q. Do you recall roughly how large he testified those would be when unzipped?
A. I believe they -- he referred to them as being several hundred gigabytes in size.
Q. Are those large files, generally speaking?
A. Those are pretty large.
MR. KAMARAJU: Let's take a look at the next --
Q. Before we go there, was the defendant logged in to his VM at the time of these searches?
A. Yes.

MR. KAMARAJU: Let's take a look at the next slide.

Q. Are you familiar with a concept known as reformatting a computer?

A. Yes.

Q. What is that, generally?

A. So, on each hard drive, there's a concept of a file system. This is what I referred to earlier, where you have the table of contents and refers to all the files on the hard drive. When you reformat a hard drive, you're essentially creating an entirely new file system, so that table of contents gets completely reinitialized; it doesn't know about any of the previous data that's on the drive.

MR. KAMARAJU: Let's take a look at the next slide.

Q. What's this?

A. So, this is a view of the, what's known as the MFT file on the defendant's C drive in the forensic program.

Q. All right. So let's walk through it. See the name at the top, dollar sign MFT?

A. Yes.

Q. What is that?

A. So, the MFT file is known as the master file table. The type of file system refers to an NCFS use of this. This is what keeps track of all the files on the file system.

Q. Do you see how all the last accessed, the file created and last-written dates are all May 5, 2016, at 11:15:57 p.m.?

A. Yes.
Q. What conclusions do you draw from that?
A. That the MFT file was created at that time due to the drive being reformatted.
Q. And which drive is this?
A. This is the C drive.
Q. Was that the Samsung SSD that you referred to before?
A. Yes.
MR. KAMARAJU: Let's take a look at the next slide.
Q. What do we see here?
A. So, this is similar. We're looking at the information for the MFT file on the D drive.
Q. And what happened to that file on May 5, 2016?
A. It was also shows -- it shows that it was created at 8:01 p.m. on May 5.
Q. What does that mean?
A. Again, with the MFT file being newly created, that would indicate that that volume was reformatted.
Q. See where it says RAID 5?
A. Yes.
Q. What is that in reference to?
A. That's in reference to what I talked about earlier. The other three drives in the computer were connected in what's known as a RAID volume or RAID 5 volume. They're hooked in a way that they're presented to the operating system as a single

drive. In this case they present as a single D drive.
Q. What was the impact of the defendant reformatting his computer on May 5, 2016?
A. You would not be able to easily access any data that was on the drive previously.
MR. KAMARAJU: Let's go to the next slide.
Q. Just to recap, let's walk through. What happened on April 23, 2016?
A. The defendant opened Eraser Portable for the first time.
Q. What happened next?
A. On April 24, the defendant ordered a SATA adapter and downloaded Tails onto his computer.
Q. Just remind us again what Tails is.
A. Tails is an operating system that directly connects you into the TOR network.
Q. What happened next?
A. So, on April 28, 2016, by this time, the defendant had used Eraser Portable to securely delete two folders on the computer -- Brutal Kangaroo and ArrayList -- and had started the process of deleting five BKP files but did not complete it.
Q. What's the next thing that happened?
A. So, on April 30, the defendant downloaded the Darik's Boot and Nuke program, which is used to securely delete hard drives. Between 10:51 and 10:55 on April 30, there were searches performed, including "how to kill your data dead with these

tips and tools" and "wipe" utilities for Samsung and Western Digital hard drives.

Q. What happened next?

A. From April 30 into May 1, so late on the 30th, the defendant periodically would unlock the screen saver to his virtual machine, indicating he was logged on. Around 3 a.m. on May 1, the defendant performed a search for "how I can verify that a one terabyte file transferred correctly." In addition, he also searched for ways to hash data.

Q. What's the next thing that happened?

A. On May 5, 2016, both drives, the C and the D drive, were reformatted.

Q. What's the impact of that?

A. That would make it difficult to recover data that would have been on those drives previously.

MR. KAMARAJU: Your Honor, no further questions at this time.

THE COURT: All right. Ms. Shroff.

MR. BRANDEN: Judge, I'll be doing the cross.

THE COURT: Mr. Branden.

MR. BRANDEN: Is now a good time for lunch?

THE COURT: No.

MR. BRANDEN: I'd like to integrate some comments that I heard from the direct testimony.

THE COURT: OK. Why don't you start. We'll break at

1:00.

CROSS-EXAMINATION

BY MR. BRANDEN:

Q. Good afternoon, Mr. Berger. I'm Jim Branden. How are you?

A. I'm all right.

Q. Good.

For the most part, I'm just going to make a review of your demonstrative and go over some of those slides, hopefully in order, so we stay in the same rhythm that the government started us off on.

MR. BRANDEN: First of all, can we see slide No. 6, please.

Q. You testified about this slide. This appears to be from Anthony Leonis, correct?

A. Yes.

Q. To Joshua Schulte, correct?

A. Yes.

MR. BRANDEN: And others are cc'd.

And may I see slide 5 as well.

Q. OK. This slide, if I'm correct, preceded the one we just looked at from Anthony Leonis, correct?

A. Yes.

Q. And in this slide, Mr. Schulte is explaining why he believes that he should still be an admin on OSB libraries, correct?

A. Yes.
Q. He's making a case for himself there, correct?
A. It appears that way, yes.
MR. BRANDEN: OK. And then if we go again to No. 6, and the body of that is in 7, I believe.
Q. And here is Mr. Leonis's response, correct?
A. Yes.
Q. Does Mr. Leonis directly say that Mr. Schulte cannot be an admin systems administrator at OSB?
A. On this slide?
Q. Uh-huh.
A. No.
Q. No. All he says, correct me if I'm wrong, is that Jojo has been brought on to manage it, correct?
A. Correct.
Q. But he doesn't say directly that Mr. Schulte cannot be the systems administrator?
A. Correct.
Q. OK. So that would appear to be still an open question, correct?
A. Based on only this slide?
Q. Uh-huh.
A. Yes.
Q. OK. Now, moving on further to the date line that you established with regard to the Vault 7 and Vault 8 release on

WikiLeaks, there are some certain limitations to the value in your report with regard to that, and I'll click them off. I believe that you would agree that the report did not purport to identify the date the data was exfiltrated from the CIA, is that correct?

A. At the time the report was written, yes, that's correct.

Q. OK. And secondly, other than the analysis of the four data points that you talked about on direct -- two of which were in Confluence, two of which were in Stash -- the report did not analyze the contents of the data on WikiLeaks to confirm with 100 percent certainty on a match to the data within the CIA DevLAN database, is that correct?

A. That's correct.

Q. And third, it was unclear, for purposes of the report, whether the times listed therein were Eastern Standard Times or not, correct?

A. At the time of the report, yes.

Q. Uh-huh. OK. So that interested me. I'm not sure that it is a pivotal point, but the window that you ultimately determined in Confluence that you found was the operable window, that the materials were taken from that 3/2, 3/3 date was from March 2, 2016 at 3:58 p.m. to March 3, 2016, at 6:47 a.m., correct?

A. Correct.

Q. And the backup was at 6:29 Eastern Standard Time, right?

A. Correct.
Q. So would the fact that you don't know whether those other times, meaning the window times, were Eastern Standard Time affect the analysis?
A. If you're asking me at the time of the report what I knew?
Q. Uh-huh.
A. At the time of the report, we didn't know what time zone the times in the database were using, correct.
Q. So what I'm saying is if there's a four-hour switch, right, from whatever Zulu time is versus Eastern Standard Time, it may be that the backup from 6:29 on March 3 does not actually fit within your window? Correct?
A. Incorrect.
Q. And why is that?
A. It has to do with how the backup files were named.
Q. I guess I'll have to take your word. I don't really know what that means. Can you just elaborate a little bit?
A. I can elaborate.
Q. Sure. Please.
A. So, Mr. Leedom testified yet about how the backups were generated on the Atlassian products. Specifically, he showed the screenshot of what was referred to as a backup script. This was a program that ran each day at a specific time to generate the backups on each system.
Part of that script was to generate the file name for the

backups. So as we've seen the screenshot several times, both the SQL and TGZ files, they had the Confluence and they had a time stamp in the file name. That was generated in the script. The way the script did that is it made a call to the system to get the current system time. It then took that time and embedded it inside the name of the file. I believe the Confluence times had that time of 0625, which I testified that indicated the beginning of the backup script, and I believe it took about three or four minutes to run. And that's why the last modified time was 6:29 a.m. Because that time is indicated in the file name and that matches the times of the files we're looking at when we're looking at them in a computer on Eastern Standard Time, we can conclude that that computer was, in fact, set to eastern time.

Q. OK. Thank you for that.

A. You're welcome.

MR. BRANDEN: Now I'd like to look briefly at slide 23, if I may.

Q. You testified at some length about this slide, and in particular, you commented on the PrevVer number, correct?

A. Correct.

Q. And that number ends in 129, correct?

A. Correct.

Q. And there were 17 versions of Michael R.'s home, and I think it's your testimony that the 17th version is the one that

appears on WikiLeaks, correct?
A. Correct.
MR. BRANDEN: And now the next page, please, 24.
Q. And here we have, I guess this is a screenshot; is that what you would call this?
A. Yes.
Q. From the WikiLeaks release?
A. Yes.
Q. OK. And it shows that this is the 17th version of Michael R.'s home and that there were 16 previous versions, correct?
A. Correct.
Q. And the PrevVer number is on this page on the line that begins with "local host," correct --
A. Correct.
Q. -- at the top?
But above that there's a separate number, which is just one number higher than the 129?
A. Yes.
Q. It's 3375130. Can you tell me why that number's there?
A. So, being as how the page was entitled "Michael R.'s Home," and it shows that on WikiLeaks's site, it seems that WikiLeaks changed it. They appear to have done that to redact the name Michael R. In doing so, they replaced it with that number that ends in 130.
Q. Now, at the time that you prepared your initial report from

which your demonstrative is drawn, you were already informed, were you not, that people at the CIA or people at the FBI believed that the leak occurred -- the leaked materials were from around March 2 or March 3? Is that correct?

A. Yeah. I was given an idea of when they thought the data was from, yes.

Q. So in a sense, your report was really just a confirmatory report?

A. It was a report to go investigate what happened and confirm it, but it wasn't that I took what they said and just put it on paper. I went and did my own investigation.

Q. And during your investigation in the matter, did you come to learn that at some point there had been a different date that was suggested for the date of the materials, the Vault 7, Vault 8 materials?

A. I had heard early on in the investigation of different dates, yes.

Q. And do you remember what that date was?

A. I think it was around March 7th or 8th, I believe.

Q. OK. So the initial date that was suggested as a possible date to WikiLeaks was March 8, but it was modified by you and others back to the 2nd or 3rd, is that correct?

A. I didn't modify anything. I didn't make that determination of March 7th or 8th.

Q. And no one has read through what's on WikiLeaks and

compared it to the materials in Confluence and Stash; it's just that you've used these data points to determine the window?
A. You mean no one's read through the data in its entirety?
Q. Yes.
A. I don't know. I have not read all 10,000 pages, no.
Q. And further, there's nothing in the report that would tie it to a particular user of Confluence or Stash, correct?
A. I don't believe so, no.
Q. Would you agree that one of the purposes of Stash is to store old versions of files?
A. Yes.
Q. So is it conceivable, therefore, that WikiLeaks could track the March 2, March 3 version from a much later backup?
A. It's a possibility, yes.
Q. And is that true also through Confluence?
A. Yes, it's a possibility.
Q. OK. So the WikiLeaks materials did not have to come from the 3/3 backup delivered to it; it could have come from a later version stored on the Altabackups, correct?
A. It's a possibility, yes.
MR. BRANDEN: Judge, how are we doing now?
THE COURT: You're doing much better, Mr. Branden. We'll break for lunch.
MR. BRANDEN: I appreciate it. Thank you.
(Continued on next page)

(Jury not present)

THE COURT: You're on cross-examination now, Mr. Berger, so don't talk to anybody on the government team.

THE WITNESS: OK.

THE COURT: Thank you.

See you at 1:30.

(Luncheon recess)

AFTERNOON SESSION

1:45 p.m.

(In open court; jury present)

THE COURT: Mr. Berger?

All right, Mr. Branden.

BY MR. BRANDEN:

Q. Mr. Berger, in your slide presentation around slide 37 -- but I don't need it -- you testified a bit about the Tor, correct?

A. Correct.

Q. And what does Tor stand for?

A. I believe it stands for The Onion Router.

Q. Do you know when it was created or where it was created?

A. I believe it was created at least 15 years ago or so by some entity of the U.S. government, I'm not sure which part.

Q. Okay. Do you know where it gets its funding?

A. I'm not sure, no.

Q. Do you know whether organizations like Facebook offer an Onion variance, a way to communicate through Onion?

A. I don't know specifically about Facebook. I do know that there are several organizations that offer a dot onion URL to connect to their services.

Q. People would want that facility to protect their privacy, correct?

A. Yes.

Q. Do you know generally whether Tor is used by privacy advocates in general?
A. I believe it is.
Q. Are you familiar with the Electronic Frontier Foundation?
A. I've heard of them, yes.
Q. Do you know whether they support the use of Tor?
A. I don't.
Q. You also testified about encrypted containers, correct?
A. Correct.
Q. Are there major vendors that support the use of encrypted containers, so for example, does Microsoft produce such a device?
A. They produce software that enables encryption, yes.
Q. What about Apple; also?
A. Yes.
Q. So there's nothing inherently nefarious or sinister about the use of such a container, correct?
A. Yes, correct.
Q. In essence what it does, it allows the user to protect the data from inspection by third parties; is that right?
A. Yes.
Q. So for example, if I have a home computer and it's going on the fritz, if I had put my vital statistics into an encrypted container, the repairer won't be able to get to that stuff; is that correct, for example?

A. Essentially, yes.
Q. You testified as to evidence that the defendant himself had downloaded an encrypted container on April 18, correct?
A. Downloaded an encrypted container?
Q. Yeah.
A. I --
Q. Used an encrypted container?
A. I believe I testified that he used an encrypted container, yes.
Q. Yeah. Did you look through his prior history before April 18 to see whether he had used such a container earlier?
A. I believe there was -- I believe there was evidence of it being used prior to that date. I can't confirm that, no.
Q. You also testified about Tails, correct?
A. Yes.
Q. Okay. Can you tell me again what Tails is.
A. So, Tails is a operating system that is designed to boot off of a piece of removable media such as a DVD or a USB drive. The entire operating system is loaded into memory. It doesn't touch the hard drive. And its main purpose is to direct all the network traffic, so anything you might be doing in your web browser, over the Tor network.
Q. Part of Mr. Schulte's job at the CIA involved collecting data stored on enemy computers; is that correct? Would you say that's fair?

A. From what I understand, yes.
Q. So given that that's part of his job description, would it have been part of his work interest in operating a system that had no persistent data, like Tails would allow?
A. It's possible.
Q. On slide 46, please. This item here in the middle section of this slide, this has multiple ports, does it not?
A. Multiple ports for hard drives or other ports?
Q. Tell me what this device would do.
A. So, it allows you to connect two different hard drives to your computer.
Q. Okay. What's the capacity of these hard drive, how much does it hold?
A. Depends on what hard drives you put into the at adapter. The adapter itself doesn't have capacity.
Q. I see. Okay. I think you testified on direct that the defendant's home computer was configured to use RAID; is that correct?
A. Correct.
Q. Given that, wouldn't it be necessary to wipe the disc clean first to use that function?
A. To use what function?
Q. RAID.
A. You are you asking if you need to wipe a hard drive prior to setting up a RAID?

Q. Yeah.
A. Generally when you set up a RAID array, it will delete whatever was on there. The RAID initiation process would render any data on the drives previously unusable.
Q. So it would be important to clean those drives beforehand if you wanted to save that data, for example, correct?
A. Correct.
Q. Are you aware that the defendant had a large movie collection?
A. I have been informed of that, yes.
Q. Okay. And in the defendant's New York apartment, he had a large amount of computer ware, did he not?
A. Yes.
Q. Did he have a lot of capacity to store these movies?
A. From what I understand, yes.
Q. With regard to Eraser Portable that you testified again, please tell me what that is.
A. That is a utility designed to securely erase files and folders.
Q. Does that leave a log of the folders that you've erased?
A. It depends on how you use the program.
Q. It can leave a log, correct?
A. It leaves artifacts based on how you use the program. Certain operations of the program will leave certain artifacts.
Q. Does it always leave these artifacts?

A. Again, the artifacts are dependent on what operations you use the program for.
Q. So, if you wanted to cover your tracks totally, maybe Eraser Portable wouldn't be the way to go, correct?
A. It's possible, yes.
Q. Slide 55, please, then 56. So these are the two folders that Mr. Schulte deleted; is that correct?
A. Correct.
Q. As far as this investigation goes, you've heard the phrase Brutal Kangaroo, correct?
A. Yes.
Q. But as to the home folder Brutal Kangaroo, you really don't have any idea what was in that folder; is that correct?
A. You mean the folder that this is referring to on the D drive, the Brutal Kangaroo folder?
Q. Yeah.
A. No, I do not know what was in there.
Q. As to array list. Have you heard that term before?
A. Yes, I have.
Q. Okay. Have you only heard that term as part of this investigation?
A. No, I have not.
Q. What is array list?
A. It's a data structure used in the field of computer science.

Q. You don't know necessarily, even though the folder is called "array list," whether it contained array list, correct?
A. That's correct.
Q. Furthermore, the title, the words "Brutal Kangaroo," you don't know those two words in combination to be classified, do you?
A. I believe they were classified. I don't know for sure.
Q. You don't know for sure. Okay. Would it be possible for somebody like Mr. Schulte to be working on some aspect of Brutal Kangaroo from his home and then bring it into the office?
A. It would be possible, yes. I don't know procedurally if that's allowed, but from a technical standpoint you can bring data from one computer to another.
Q. And then once that information is safely within the CIA, it would be important for him to delete the home version of that folder, perhaps?
A. If that's what he wanted to do, yes.
Q. You also testified about the deletion of data and the confirmation of transferred data, correct?
A. I believe you're referring to the Google searches?
Q. Yeah.
A. Yes.
Q. Okay. And again, deleting files, there's nothing sinister about doing that?

A. Just generally deleting files, depends on what the files are, but yes.
Q. And wiping a drive clean is a common procedure for most people; is that correct?
A. I wouldn't say most people. It depends on the type of user.
Q. Okay. And you testified about the use of DBAN. Correct?
A. Yes.
Q. And are you familiar with the fact that Best Buy and Staples recommend DBAN before disposing of a disc?
A. I'm not familiar with that, no.
Q. Are you familiar with the -- are you aware that MacOS has a disc wipe option?
A. Yes, I am.
Q. Okay. Window also has a disc wipe option, correct?
A. Correct.
Q. With regard to slides 70 and 71, please. I think you described 70 and 71 as evidence that the defendant had reformatted his computer, correct?
A. Correct.
Q. Do you know if this was definitely a reformatting or is the defendant just upgrading hardware and installing new file systems?
A. You wouldn't upgrade your file system when you're installing new hardware. This is a reformat because it shows a

creation of the MFT. This -- the MFT is the underlying basis for your file system. Even if you were to upgrade to a newer version of Windows, let's say, that would not create a new MFT. The only thing that would trigger the creation of a new MFT would be reformatting the system.

Q. Throughout -- you see we're getting near the end of these slides, so I have some general followup questions for you.

Throughout your investigation, have you found any evidence that the defendant copied the Vault 7 or 8 data on to his home computer?

A. Not directly, no.

Q. Okay. Have you found any evidence that the defendant brought hard drives home from the CIA?

A. No.

Q. Have you found any evidence that the defendant plugged any hard drives from the CIA into his home computer?

A. No.

Q. Do you have any evidence that the defendant ever took data from the CIA home to put it into his home computer? Essentially the same question, again.

A. No.

Q. Do you have any evidence that the defendant stored Confluence on his home computer?

A. No.

Q. How about Stash?

A. No.
Q. Or the Atlassian suite, for example?
A. No.
Q. Do you have any evidence that Altabackups was stored on his home computer?
A. No.
Q. Do you have any evidence that the Confluence backup accessed allegedly on 4/20 was ever stored on the defendant's home computer?
A. No.
Q. Then finally I have one question that's just something of a hypothetical. But, mostly you testified with regard to the home computer stuff, those dates concerned April and May of 2016. Correct?
A. Correct.
Q. Okay. Did you become aware that the defendant left the CIA at some point?
A. Yes.
Q. Do you know when that was?
A. I believe approximately October, November of 2016.
Q. Did he relocate?
A. Yes, I believe he did.
Q. Where did he move to?
A. He moved to New York.
Q. And did he get a new job?

A. Yes.
Q. Okay. And when was the search of his New York apartment?
A. It was some time in March of 2017 I believe.
Q. Is it your suggestion that the devices from his home that you searched and analyzed are the same devices that he had in Virginia, a year earlier?
A. The devices were found in the defendant's apartment.
Q. Okay. If someone had something really terrible in their devices in their home computer, and they were moving to a whole other place, would it have been more advisable to just destroy that home computer and all removable media, and buy new stuff when you get to New York? Would that have been a safer, more prudent thing to do?
A. If they had reason to believe that there was evidence of that on those drives, sure.
MR. BRANDEN: That's all I have, Judge.
THE COURT: Mr. Kamaraju.
MR. KAMARAJU: Just a few questions, your Honor.
REDIRECT EXAMINATION
BY MR. KAMARAJU:
Q. Do you remember Mr. Branden asked you about whether you reviewed the entire leak page by page?
A. Yes.
Q. He asked you some questions about reviewing two data points?

A. Yes.
Q. To arrive at your ultimate conclusion, did you only look at two data points?
A. No.
Q. Did you do any analysis of the rest of the leak?
A. Yes.
Q. Can you describe for the jury what you did.
A. So, we looked at several data points. We looked at pages that were in the leak and we looked at their corresponding records in the database. We found that there was a -- it started to form a pattern. There were data that was in the database that was on WikiLeaks, and there was data in the database not present on WikiLeaks.

We then looked at the distance between those points, and then we started to move to points that were closer and closer together. We then arrived at a set of two points for each system, Atlassian, the Atlassian Confluence product and the Stash product. We picked the two points that were closest together from either side of the line. The line being the division between data from the databases that was on WikiLeaks, and data that was not on WikiLeaks.
Q. Did you do anything to determine whether there was any data released by WikiLeaks that came after March 3, 2016?
A. Yes, we did.
Q. Can you describe for the jury what you did.

A. One of the things that we did was look through the content of the pages that was present on WikiLeaks, and we searched the text of those pages for dates in different formats.

You can have a date that is a two-day month, two-day day and a four-day year. You could have a date format that starts with a four-day year, then the month and the day. Two digit year. So there is several variations of how people document dates.

We looked at several of those and ran searches for dates with the year 2016, 2017, through the WikiLeaks data.

Q. After you did that, is your opinion still that the data comes from the March 3, 2016, time period?

A. Yes, it is.

Q. You remember Mr. Branden asked you about whether it was also possible that data came from a later backup; do you remember that?

A. Yes.

Q. You said it was a possibility, right?

A. Yes.

Q. Do you think that's what happened here?

A. No, I don't.

Q. Why not?

A. Two primary reasons. Number one, Mr. Leedom testified yesterday about what the reconstruction process would have been like if you had taken the backup from Confluence and tried to

reconstruct pages that were displayed on WikiLeaks. He also explained how due to an error with the backup script, there was corruption in parts of the Confluence database that would have made it exceedingly difficult to reconstruct everything.

If you wanted to go and take that data and then roll it back to earlier versions to make it, let's say, look like a previous version, that would have been another added layer of complexity on an already hard process.

The second reason is my understanding of how WikiLeaks works, which is they like to publish lots of data. If they had data in their possession from a later date, and only released data up to a previous point in time, that would mean that in their possession they have that additional data that they have not put out.

Q. Do you remember you were asked about whether you knew what was in the Brutal Kangaroo and array list folders on the defendant's computer?

A. Yes.

Q. When you looked at the forensic image of the defendant's home computer network, could you access those folders?

A. No.

Q. Why not?

A. Because they had been deleted.

Q. What had they been deleted with?

A. Eraser Portable.

Q. Does that mean they were securely erased?
A. Yes, it does.
Q. You were also asked a series of questions about whether you found evidence of Confluence on the defendant's computer or the Altabackups on the defendant's computer; do you remember that?
A. Yes.
Q. You remember testifying about the defendant reformatting his computer?
A. Yes.
Q. What would that do to the data that was on his computer prior to the reformat?
A. When you reformat, you wipe away the existing file system and you build a new file system on top of that. Anything that was there is now available to be overwritten. So over time, files would get overwritten that were not part of the new file system.
Q. Do you remember Mr. Branden asked you some questions about the initial report that you put out?
A. Yes.
MR. KAMARAJU: Ms. Hurst, can we pull up Government Exhibit 1207-27 and 30, please. For 1207-27, let's just blow up the area around the government exhibit and header. I think you've done a bunch before. Thank you.
Q. At the time of your initial report, had you seen Government Exhibit 1207-27?

A. I had not.

MR. KAMARAJU: Can we do the same thing for 30, please.

Q. How about 1207-30. At the time of your initial report had you seen this exhibit?

A. I had not.

Q. Prior to your testimony, have you seen these exhibits?

A. Yes.

Q. Does Government Exhibit 1207-27 and 1207-30 change your conclusion that the data on WikiLeaks was dated March 3, 2016?

A. No.

Q. What, if any, impact on your opinion do these two exhibits have?

A. It confirms the results of the -- the data that's in the report, and it allows me to draw an opinion that the data came from that backup file, the March 3 backup file.

Q. Why is that?

A. Because the data in the backup file would fit within the window that was defined in the report.

MR. KAMARAJU: One moment, your Honor. No further questions your Honor.

THE COURT: You're excused. Thank you very much.

(Witness excused)

THE COURT: Call your next witness.

MR. LAROCHE: The government calls Bonnie Stith, your

Honor.

THE DEPUTY CLERK: Please state your name for the record.

THE WITNESS: Bonnie Bennett Stith.

(Witness sworn)

THE COURT: All right, Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

BONNIE BENNETT STITH,

called as a witness by the Government,

having been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. LAROCHE:

Q. Good afternoon, Ms. Stith.

A. Good afternoon.

Q. Have you worked at the CIA?

A. I have.

Q. For approximately how long did you work at the CIA?

A. 34 years.

Q. Do you work there anymore?

A. I do not.

Q. Why don't you work there anymore?

A. I retired.

Q. When did you retire?

A. I retired the 3rd of January, 2017.

Q. Prior to your retirement, what was your position within the

CIA?

A. Immediately prior to my retirement, I was the director for the Center for Cyber Intelligence.

Q. When did you become the director of the Center for Cyber Intelligence?

A. September 2015.

Q. Does that go by CCI?

A. Yes, it does now. It was Information Operations Center at the time.

Q. What is CCI?

A. CCI is the Center for Cyber Intelligence. It is the -- I would say the premier cyber collection organization of the U.S. government, but certainly of the CIA.

Q. Is the director position the highest ranking position within CCI?

A. It is.

Q. Generally, what were your responsibilities as director of CCI?

A. My general responsibilities were to set the vision, establish priorities, oversee the progress towards collecting better intelligence faster, and managing up and out towards modernization, which was a reorganization going on at the agency.

Q. When you were director of CCI, approximately how many employees did you oversee?

A. Several thousand.

MR. LAROCHE: Can we bring up Government Exhibit 89, please.

Q. You see CCI at the top of this exhibit?

A. Yes.

Q. There is the Engineering Development Group below that; do you see that?

A. Yes.

Q. Was that the only group that you oversaw?

A. No.

Q. Approximately how many other groups did you oversee?

A. In excess of 14.

Q. Are you familiar with the position developer?

A. Yes, I am.

Q. Just generally, what is a developer?

A. They write code to help us develop the capabilities to access cyber means to get to intelligence.

Q. About how many levels of management were between you and a developer?

A. Could have been six, could have been seven, could have been eight.

Q. How many times as director of CCI did you deal with a dispute among developers?

A. Only once.

MR. LAROCHE: We can pull that exhibit down.

Q. Who was that dispute between?
A. It was between Amol and Josh.
Q. Josh --
A. Josh Schulte.
Q. Did you become aware of that dispute in about March 2016?
A. Yes, I did.
Q. Prior to that time, had you any interactions with those individuals?
A. I don't recall ever interacting before that time.
Q. How did you learn about the dispute between them?
A. I learned that there had been an exchange of words between a couple of developers that I viewed as unprofessional behavior, and it had resulted in some disruption in that branch.
Q. After learning of that dispute, did you meet with the defendant and Amol?
A. I did.
Q. Did you meet with them separately or together?
A. Together.
Q. At the time, did you have an understanding that the defendant had alleged that Amol threatened him?
A. I did.
Q. Why did you decide to have the meeting together?
A. It had been investigated by the threat management unit, and I had talked to the leadership involved, and there didn't seem

to be any foundation to that.

Q. Approximately when did the meeting occur?

A. It would have been in March. Some time after that.

Q. Did you have any difficulty getting the defendant and Amol to come to that meeting?

A. I did.

Q. What was the difficulty?

A. Josh did not want to meet with Amol. He said that he was afraid of Amol, and that he didn't want to be in the same room meeting with him.

Q. Did he come to the meeting?

A. He did.

Q. Why?

A. Because I insisted.

Q. During the meeting, what, if anything, did you say to them?

A. The meeting was really about me telling them what I expected of them as employees of the U.S. government, as employees of the agency, and as really, what I considered to be stewards of the public trust in the space that we were in.

I talked to them about responsibility for what they were supposed to be doing, about the honor that we had as people that got to work for the agency, and about the obligation that we had to our nation.

(Continued on next page)

MS. SHROFF: I'm sorry. I missed the last part.

THE WITNESS: The obligation that we had to our nation.

MS. SHROFF: Thank you.

BY MR. LAROCHE:

Q. How did Amol react to that?

A. Amol, I think, was chagrined at having to be there. He seemed -- I don't -- it wasn't usual for a developer to come before the director in that space, so I think he was embarrassed.

Q. What about the defendant?

A. Josh didn't really exhibit much emotion.

Q. Do you recall whether the defendant said anything during that meeting?

A. I don't recall.

Q. After you met with the defendant and Amol, were they moved within their branch?

A. Yes.

Q. Were you consulted on that decision?

A. I don't recall directly, but probably.

Q. And why do you say that?

A. I think we had made the decision at that point that they needed to be separated, so --

Q. Why?

A. We needed the work to continue, and if they couldn't

continue working in the same space, then they needed to be separated so they could continue to work.

Q. And why did you need the work to continue?

A. The motto of the Center for Cyber Intelligence is "we can produce better intelligence faster." Our nation depended on us to do that, and we had important work going on. And at the very foundation of the cyber effort is the code writing and the tool development that goes on, and I needed them to be focused on that job.

Q. Now, did there come a time when you learned that the defendant had filed a protective order against Amol?

A. I was briefed on that, yes.

Q. In your experience at the CIA, are you aware of another time where that's happened between two agency employees?

A. No.

Q. What, if any, action was taken as a result of that protective order?

A. I think at that point -- well, we called in threat management unit again. We also called in security because it was, it was so unusual to have agency employees in a local court for those issues that there was another investigation that was, I think, started. But also, I think we then separated them even further.

MR. LAROCHE: Could we pull up Government Exhibit 1046, please, and go to the second page. And just zoom in on

the bottom email, please.

Q. Who sent this email?

A. Deborah.

Q. And who did she send it to?

A. She sent it to Amol and Josh.

Q. And why did she send this email?

A. To inform them they would be moving into different cubicles.

MR. LAROCHE: Let's go up to the next email. Maybe just go up one more slide and see who sent it.

Q. This is on March 29, is that correct?

A. Uh-huh.

Q. Who sends this email?

A. Anthony.

Q. And who did he send it to?

A. He sent it to Amol and Josh and carbon copied Michele, Susan and Dana.

MR. LAROCHE: Let's go to the next slide.

Q. Are you copied on this email?

A. I am.

Q. Who else is copied?

A. John, Karen, Michael, Anthony, Deborah and Sean.

Q. Do you see in the first sentence it says, "After further consultations with HR, security and the CC front office"?

A. The CCI front office, yes.

Q. Do you have an understanding of what that's referring to?
A. We had a meeting to discuss what was going on, and a decision was made that they would be separated.
Q. Why is that?
A. At that point I think there was a restraining order granted, and so, in order to continue working, we wanted them in different places.
I also did not believe that one should be moved and not the other. Because it was unclear as to really what was going on, I thought both of them should be moved.
MR. LAROCHE: Let's go to the next email, please. Just zoom in on that, please.
Q. We're still on March 29, is that correct?
A. Yes.
Q. Who sent this email?
A. Anthony.
Q. Sorry. At the top there, on the "from"?
A. Oh, I'm sorry. It was from Josh.
Q. That's OK.
A. It was to Anthony.
Q. And did he copy all the same folks as before?
A. Yes.
Q. And do you see that on the copy line, and this person was on the last email, is Karen?
A. Yes.

Q. Who is Karen?
A. Karen -- that was Karen. She is the group chief.
Q. And if we could just read that sentence, please?
A. "I just want to confirm this punishment of removal from my current branch is for reporting to security an incident in which my life was threatened and/or for resubmitting a protective order against Amol."
Q. And you said you were involved in those consultations about the move, is that correct?
A. Yes.
Q. Was that move punishment?
A. No.
Q. Why not?
A. Based on what was going on, we felt it was in everybody's best interests to have them separated, and if we were going to move one, it seemed the other should be moved as well. And since there was no clear-cut case for what was going on, we opted to move them both.
MR. LAROCHE: Let's go to the next email.
Q. And this is still on March 29, is that correct?
A. Yes.
Q. And who sent this email?
A. It was Josh.
Q. Did you receive this email?
A. I did.

Q. If you can just read the first two sentences, please.
A. "I was told that there would be no written response to my email, so I'm proceeding with my move, assuming it is directly due to with my security report."
Q. Did you tell the defendant that there would be no written response to his email?
A. No.
Q. Are you aware of anyone else telling him that?
A. No.
MR. LAROCHE: We can pull that down.
Q. Now, after this email exchange, did there come a time when you learned about a hearing related to the protective order between Josh and Amol?
A. Yes.
MR. LAROCHE: Let's pull up Government Exhibit 1051, please, and if we can just look at the bottom.
Q. Do you see there's an email dated April 6, 2016, at 3:35? This is at the far bottom.
A. At the far bottom, yes.
Q. Is that an email from Josh?
A. Yes, it is.
MR. LAROCHE: Let's go to the next slide, please.
Q. And just who did Josh send this email to?
A. He sent it to Michele, to Susan, to me, to Michael and to William.

Q. Now, had you reviewed this email before your testimony today?
A. Yes.
Q. And just generally, what does the defendant address in this email?
A. The protective order that he had filed against Amol.
Q. Was it typical for you to receive emails like this from developers?
A. No.
Q. How many emails like this did you receive from developers while you were director of CCI?
A. Only from Josh.
Q. Can you go to the first sentence of this -- I'm sorry. Read the first sentence.
A. "Today was the hearing for the protective order I filed against Amol."
Q. Were you present at that hearing?
A. No, I was not.
Q. Are you aware of what happened at that hearing?
A. No.
MR. LAROCHE: Let's go to the, zoom in on the second paragraph, please.
Q. See where there's a reference to EAP?
A. Yes.
Q. Just generally, what is EAP?

A. EAP is the agency's employee assistance program. We have psychologists. We have financial counselors. There's all kinds of resources for people that are having issues going on of any type, and so, it is a resource for agency employees. They can self-refer or otherwise.

Q. Do you see the sentence starting "therefore," the second from the bottom?

A. "Therefore," yes.

Q. Can you read that?

A. "Therefore, someone in my management chain clearly told Amol about my second appointment."

Q. And just read it to the end.

A. "Why? Why is information that I thought confidential being shared with Amol?"

Q. Did you share any information about EAP with Amol?

A. No.

Q. Are you aware whether or not anyone else did?

A. No.

MR. LAROCHE: If we can zoom out again and zoom in on the paragraph starting Bonnie.

Q. Let's just read the first sentence, please?

A. "Bonnie, I'm very concerned with EDG and chief EDG's handling of this incident, and I'm hoping you can help me."

Q. Just pause there for a second. You see the C forward slash EDG; do you have an understanding of who that refers to?

A. Karen.

MS. SHROFF: I'm sorry?

MR. LAROCHE: I believe the witness said Karen.

Q. Is that correct?

A. Yeah, it would have been Karen, the chief of EDG.

Q. Let's continue reading from the "I know you don't."

A. "I know you don't want to be involved with this, and I'm sorry it took place under your management. But I am running out of upper management and HR people to inform. From the onset of this entire situation, I have only wanted to be taken seriously and treated fairly, neither of which has happened."

Q. Do you agree that he wasn't taken seriously with respect to this complaint?

A. No.

Q. Why don't you agree with that?

A. The fact that I met with him; the fact that I was being briefed on them; the fact that this was an ongoing situation. We were all taking it very seriously. We had threat management unit involved. We had security involved. People were looking into this to make sure that there wasn't something else going on.

MR. LAROCHE: We can zoom out and go to the next paragraph, please.

Q. And just read the first sentence.

A. "My life was threatened by Amol, and I seriously felt he

may kill me or others."
Q. As director of CCI, what steps would you have taken if you believed someone was going to kill someone at CCI?
A. They wouldn't have been at work.
Q. Did you take those steps with respect to Amol?
A. No.
Q. Why not?
A. We had an investigation, and the investigation did not merit that.
Q. If we can go to the last sentence that starts "despite."
A. OK. "Despite Amol admitting his actions on 3/1 to security, I felt that the issue still wasn't taken seriously."
Q. Do you have an understanding of what he's referring to by "admitting his actions on 3/1 to security"?
A. No.
MR. LAROCHE: If we can go to the next line at the bottom.
Q. Just read that sentence, please.
A. "From the time I reported the incident, chief EDG has still never sat down and talked to me."
Q. Again, who is that a reference to?
A. Karen.
MR. LAROCHE: Let's go to the next page, please, and just zoom in on the top paragraph.
Q. Just continue reading the end of that sentence.

A. "Was no discussion of safety in the workplace or my concerns of working directly with Amol."

Q. And then the next sentence.

A. "I was told to go back to work, and despite my concerns to management of working next to Amol, I was told there were no seats to move us."

Q. Did you tell the defendant to go back to work during your meeting?

A. No -- well, yes, I did tell him to go back to work.

Q. Why?

A. Because what we do is important. And again, there had been no indication that there was a real threat there. My feeling was go back to work and focus on what's important.

MR. LAROCHE: Let's zoom out again.

Go to the next paragraph, please.

Q. Do you see there's a sentence that starts -- sorry. Read until the "my management" in the second line.

A. "At some point I sat down directly with you, Bonnie. You told me I didn't have to worry about losing my job over this. Perhaps you can see my frustration in all this. My management, specifically Karen, has fundamentally failed to ensure my own safety, and now I feel my management is informing Amol of information that he does not need to know. I'm very upset with all of this and feel that management's only concern is CYA and not their employees."

Q. Did you agree with the assertion that Karen had failed to ensure the defendant's safety?
A. No.
Q. Why not?
A. Again, we'd called in security. People had been interviewed. There'd been an investigation of what was going on, and there was nothing found.
Q. And did you agree with the assertion that management's only concern was CYA?
A. No.
Q. Finally, can you please read the last paragraph.
MR. LAROCHE: We can zoom out and then zoom in.
A. "More than anything, I want this situation to go away. But as I still feel I'm being punished and my management does not have my back and that confidential information is told to Amol, how can I feel any level of trust from my management? I sincerely hope you can assist me."
Q. Did you respond to this email?
A. I believe I did.
MR. LAROCHE: Let's take a look at the response on the first page. If you could just zoom in on that, please.
Q. When did you send this response?
A. April 6 at 7:27 p.m.
Q. Is that the same day you got the email?
A. I think it would have been.

MR. LAROCHE: We can just zoom out and show you the bottom.

A. Yeah. OK.

Q. Could you please summarize what you said in response?

A. I told Josh I'd seen his note and I had read it, and I wanted to reassure him that we were taking it very seriously. And to my knowledge, no confidential information had been shared with anybody regarding any appointments or conversations that anyone had had with EAP.

Q. You testified that you disagreed with some of the things that the defendant said in his email to you?

A. Yes.

Q. Why didn't you address those in response?

A. They weren't worth addressing. What I wanted was for him to focus on what was supposed to be the most important thing going and off the rest of this stuff. It seemed like there was a constant distraction going on.

MR. LAROCHE: Let's just zoom back out and then zoom in on the defendant's response.

Q. Do you see you received this the next day, on April 7? Is that right?

A. Yes.

Q. Can you please read what the defendant said in response.

A. "Thank you. I'm hoping to focus on the Vortex and other tool rewrites for the remainder of the week and ignore all the

rest of the noise."
Q. What was your reaction to that?
A. I was relieved.
Q. And why?
A. I was writing notes at 7:56 at night. My day went from about 8:00 to about 5:00 with back-to-back meetings, and with everything else going on, this was a lot. I mean, I felt for what was happening here, but there was a lot of other stuff going on. I wanted Josh to settle down and get to work.
Q. Was that the last time you became aware of a problem with the defendant?
A. I don't recall.
Q. Did you later learn about issues with the defendant's privileges to a computer system?
A. Yes.
Q. And how did you learn about that?
A. I was briefed. They had switched jobs. And when you switch a job at the agency, typically you lose access to the things you were doing before and they move you to another project and grant you accesses to that project. What was happening was that Josh was going back and recreating his accesses back into the area he was before.
Q. Now, did you have any involvement in dealing with those issues?
A. Other than being briefed and making sure that they were

being documented, no.
Q. And who was principally responsible, generally, for dealing with those activities?
A. At that point it was Mike.
MS. SHROFF: I'm sorry?
THE WITNESS: Mike.
BY MR. LAROCHE:
Q. And was he part of management?
A. He was. At that point I think he was the acting chief.
Q. Of what part?
A. Of EDG.
Q. Of EDG?
A. Uh-huh.
Q. Now, earlier you said that one of the things you conveyed was you wanted Amol and the defendant to just get back to work, is that right?
A. Yes.
Q. Why did you want them to do that?
A. Back to the responsibility we have to the public that's paying us to keep them safe. And again, we've created a culture in the organization that was really about moving forward in an innovative way. This kind of nonsense got in the way of a working environment for their colleagues and for the rest of us, so we needed that job done.
Q. And what would happen if developers weren't able to do

their jobs?
A. Well, they probably shouldn't call us the cyber center anymore. We had to be something else, because that was a key piece of what went on in that organization.
Q. What impact would that have had on your mission?
A. We wouldn't have been able to complete our mission.
MR. LAROCHE: No further questions, your Honor.
THE COURT: Ms. Shroff.
CROSS-EXAMINATION
BY MS. SHROFF:
Q. Did you say the culture of the mission was to be moving forward in an innovative way?
A. Yes.
Q. How many levels removed were you from EDG?
A. EDG was one of the groups that I supervised and led.
Q. And how many groups did you lead?
A. More than 14.
Q. And in more than 14 groups, were you aware that in this particular group, grown men flicked rubber bands at each other?
A. At the end of the day --
Q. Just during the time it was going on, not --
A. No, I was not.
Q. OK. Were you aware that grown men had Nerf guns and were shooting at each other?
A. No.

Q. Were you even aware that in one of your 14 branches there were grown men with Nerf guns? Not one grown man, grown men.
A. It was a group. No.
Q. Were you aware that there were people shoving each other into desks?
A. No.
Q. Were you aware there were people hitting each other? Grown men, men of the age of 30, hitting each other.
A. No.
Q. Wasn't that the culture of EDG that you were completely unaware of in April of 2016?
A. Yes.
Q. Right.
And who supervised these grown men?
A. Chief EDG.
Q. And who, pray tell, was chief EDG?
A. Karen.
Q. And she was responsible for supervising these individuals, correct?
A. Karen was the group chief.
Q. Was she in charge of supervising them, ma'am?
A. She was their group chief.
MS. SHROFF: I'll take that as a yes.
Q. Did Karen ever come to you and say, I have these bunch of grown men acting like this, help me?

A. No.
Q. Let me ask you a question. Was there an intermediary boss between you and Karen?
A. No.
Q. Was there an intermediary boss between Karen and these EDG developers?
A. Yes.
Q. And who, pray tell, was that?
A. There probably were a couple of levels. Sean was his immediate boss.
Q. You had not a clue, did you, that any of this was going on because Sean never, ever told anyone else? Correct?
A. I can't speak to that.
Q. Well, certainly you never heard from Karen that this was going on, correct?
A. No.
Q. Would you say that the EDG group was an important group for the CIA?
A. Yes.
Q. Tell them. Why was it important?
A. Those are the tool writers.
Q. Right.
A. They developed the capabilities.
Q. And they are the coders and the developers, correct?
A. Yes.

Q. And supervising them is an important job, correct?
A. Yes.
Q. As you said, it contributes to your mission, right?
A. Yes.
Q. And until one of the coders brought it to your attention, you were clueless? Yes or no.
A. Yes.
Q. And it was, in fact, the coder that brought it to your attention, right?
A. I don't recall him ever bringing that to my attention.
Q. Really? It wasn't Mr. Schulte who filed a complaint? He's a coder, right?
A. The complaint wasn't about rubber bands and Nerf guns.
Q. I didn't ask you that. My question was, who brought on the complaint?
A. Mr. Schulte filed a complaint --
Q. Right.
A. -- about --
Q. And Mr. Schulte filed a complaint about the way he was being treated by Amol, correct?
A. Yes.
Q. And when he felt his complaint wasn't taken seriously, he escalated it, right?
A. Yes.
Q. And nobody wanted it escalated, right? Well, Karen

certainly didn't want it escalated, right?
A. She never told me that.
Q. Well, did she escalate it?
A. I was briefed on it.
Q. No, no. That wasn't my question. Of course, you were briefed on it. You were briefed on it because he wouldn't stop, correct?
A. Yes.
Q. He kept escalating it. He escalated it, right?
A. He escalated it.
Q. Right. He felt he wasn't being treated fairly, correct? Whether you agree with it or not, he felt his life was threatened, correct?
A. Yes.
Q. He went and got a protective order in a courtroom, correct? State courtroom, correct?
A. Yes.
Q. By the way, did you know at some point that people had actually gone to court?
A. I was briefed on the fact that they had gone to court.
Q. Did somebody get a transcript and see what was said in that proceeding?
A. It was handed to our security.
Q. OK. Let's go with that. Did security get you a transcript?

A. No.
Q. You have two CIA employees going to a state court, correct?
A. Uh-huh.
Q. This is the last thing the CIA wants, am I right?
A. I don't know that I'd call it the last thing, but it's not something that was done.
Q. I mean, isn't it fair to say no company wants that headache? Right? Private, public, government, nobody wants that, right?
A. I can't speak to that.
Q. OK. Well, you didn't want that, did you?
A. It wouldn't be my first choice, no.
Q. OK. And security was in charge of this, correct?
A. It was handed over to security.
Q. Right. Security never got you a copy of the transcript, correct?
A. No.
Q. You have no idea what was even said by Amol in open court, correct?
A. No.
Q. You have no idea if Amol actually told the judge that this man has been sent to counseling, correct?
A. No.
Q. You do not know how Amol got that information, sitting here to this day, correct?

A. No.
Q. And yet you think you knew the culture of EDG in April of 2016?
A. Yeah --
MS. SHROFF: I withdraw that.
Q. Let's just go back to the state complaint, shall we?
Did you, by any chance, ever find out how Amol knew he was referred to therapy?
A. No.
Q. Did you ever try and tell Karen: Hey, you know, we may want to find out why these two people who are at each other know information that is upsetting to one developer, that is personal to one developer, how does Amol know this? Did you ever ask?
A. No.
Q. Do you recall a time when Karen ever tried to tell you how Amol got that information?
A. No.
Q. Do you recall getting the Same Time chat or ping, whatever it is that it's called, about Amol having information about Mr. Schulte?
A. No.
Q. And it's fair to say that sitting here today you still don't know how Amol got that information, right?
A. No.

Q. Now, you testified that there came a time that you sat down and you had a meeting with these two individuals, right?
A. Yes.
Q. And is it fair to say that at the time you sat down with them, you didn't really know whether they liked coding or they didn't like coding? Right? Is that fair to say?
A. Yes.
Q. You just had these two problem people who were in your office, right?
A. Yes.
Q. You did not know whether one, Amol, didn't mind if he was no longer a coder, correct?
A. No.
Q. You didn't know if Amol's end goal in life was to be in management and no longer be a coder, correct?
A. No.
Q. In fact, you didn't even know that Amol wanted to be in management, correct?
A. Nope.
Q. OK. So just hypothesize with me that Amol didn't care about being a coder. Fair to say, then, he wouldn't be upset about being moved out of EDG, correct?
A. I can't speak to that.
Q. Well, you're the boss. You said you knew the culture. You tell me.

A. I can't speak to Amol's intentions or his thoughts.
Q. OK. Well, did you know what Amol's goals were at that time?
A. No.
Q. Did you know Amol wanted to anyway leave EDG?
A. No.
Q. Did you know if he cared about remaining in EDG?
A. No.
Q. How about Mr. Schulte; did you know if he cared about remaining in EDG?
A. No.
Q. Did you know if he wanted to leave EDG?
A. No.
Q. Did you know if it would have mattered to him if he left EDG?
A. No.
Q. So it's fair to say that an action taken against two people would have a different effect on two people, correct? You said you moved both --
A. Yes.
Q. -- right?
Amol seemed unconcerned and just embarrassed at having to be there at all, correct?
A. They were both moved within EDG.
Q. I understand that. One was moved to RDB and one was moved

to some mechanic group. I'm sorry. I've forgotten that acronym. You will have to forgive me.

They were moved to different groups, right?

A. They were moved to different branches.

Q. Branches, yes.

A. Yes.

Q. I keep getting that wrong.

They were moved to different branches, right? You have no idea, sitting here today or back in April, whether it mattered to either one of them which branch they were sent to?

A. No.

Q. Right. And it was decided that both should be moved because management thought that even-steven was the best way to go, correct?

A. Yes.

Q. That's what was best for management, correct?

A. That's what was best for the environment in which they were both in.

Q. Well, did you separately ask each one of them if it would matter if they were moved? No, right?

A. No.

Q. Did you ask any one of them if they were truly invested in the projects that they were working on that they didn't want to leave?

A. No.

Q. Did you ask them, Hey, listen, have you been working on something for a very long time that would upset you if you were taken off of that project?
A. No.
Q. OK. And you also testified -- I just want to shift gears for one minute before I forget my train of thought. You testified it was normal to take over access when somebody's moved, correct? Normal practice --
A. Yes.
Q. Standard operating procedure, so to speak; yes?
A. Yes.
Q. OK. Do you know when they moved these two individuals whether either or both of them took with them any part of their work with them?
A. No.
Q. Did you know whether or not they took any part of a tool that they were working on?
A. No.
Q. Did you know what tools either one of them was working on?
A. No.
Q. Did you know if somebody sat down and said: Hey, you know what? You're moving projects, but we're going to let you take some of your projects with you so that you can continue working on them?
A. No.

Q. Imagine that one of them, or both of them, were told that. Then the standard operating procedure of removing access across the board would not -- or possibly would not -- make sense, correct?

A. I can't speak to that.

Q. Now, you were shown, on direct, this --

MS. SHROFF: May I please have 1046 on the screen.

Q. And if we could just look at the "from" line, the top line, that was read to you before. Ready? Up there. Do you see that?

A. So, "I was told there would be no written response to my email, so I'm proceeding with my move, assuming it is directly due to my security report."

Q. And then the next line says?

A. "If this is not the case, then please reply."

Q. OK. And I just want to make sure, because we went through these -- everybody, all three of us have a rapid pace of speech.

THE COURT: Just ask the question.

Q. This email was not sent to you, correct?

A. No, it was not.

Q. OK. So the email was sent to Mr. Leonis, correct?

A. Yes.

Q. And do you, by any chance, know if Mr. Leonis replied?

A. No.

Q. You don't know, or no, he didn't reply?
A. I don't know if he replied.
Q. OK. And you didn't reply because you were just carbon copied on it, correct?
A. Yes.
Q. And there are a lot of people that this man carbon copied, correct? I mean, not carbon copied. I apologize.
A. Cc'd.
Q. Electronically copied, right?
A. Yes.
Q. So you do not know if, in fact, that statement or that clause is accurate or not, correct?
A. No.
Q. You don't know?
A. I don't know.
Q. Right. So it could be that he was told that there would be no written response, correct?
A. Yes.
Q. And it could be that he wasn't told that, correct?
A. Yes.
Q. It's an equipoise. Nobody knows.
OK. And then it says, "I'm proceeding with my move, assuming it is directly due to my security report." What security report is he talking about?
A. I don't know.

Q. And then it says he is going to be leaving early today, can't complete his move, and he will complete the process tomorrow, right?

A. Yes.

MS. SHROFF: OK. May I just see the bottom part of this email. No, no. The middle part. I'm sorry.

Q. See that part where it says, "I just want to confirm this punishment of removal from my current branch is for reporting to security an incident in which my life was threatened and/or submitting a protective order against Amol, "correct?

A. That's what he wrote.

Q. That's what he wrote. And you said you did not agree that there was any indication that his life was threatened, correct?

A. I did not agree.

Q. Right. You did agree, though, that somebody had a protective order, right?

A. They'd gone to court.

Q. Yes, that's right. So you knew there was a protective order?

A. Yes.

Q. And do you know if anybody replied to this email of his?

A. I don't know.

Q. OK. Fair enough. And again, this email is not directed at you; you're just copied on it, correct?

A. Yes.

Q. And then if you keep going down, that is just both of these individuals being informed of the change, correct? There's nothing more to it that involves you, right?
A. Yes.
Q. OK. Now, there comes a point when you, in fact, are emailed, correct, directly by Mr. Schulte?
A. Yes.
Q. And these emails that were 1046 are dated March 29, correct? And then the one he sends to you is April 6. There's a short gap, right? It's not long, but it's a gap, is that right? Do you have it?
A. I don't -- I'm not looking at those ones right now.
Q. OK. No. You're right.
Is hard copy better for you?
A. Fine.
THE COURT: The screen doesn't seem to be able to catch up with you, Ms. Shroff.
MS. SHROFF: Oh, here it is. 1046's up. There you go. All right.
Q. Do you see he sends you this long email, right?
A. Yes.
Q. Except the last two pages?
A. Yes.
Q. Right. And at this point, he has involved somebody above his own boss, Sean and Karen, right?

A. Yes.
Q. And he's telling somebody that the reason he is going above Karen is because, at least according to his state of mind, Karen isn't listening to him, correct?
A. Yes.
Q. OK. And he says something about moving desks?
A. Well, that's when they were moving to separate branches, I think.
Q. Right. And he says that he was told that he had refused to move desks and that he disagreed with that statement or that accusation, correct? He's telling you he thinks it's not true?
A. Yes. I'm looking at this note.
Q. Correct?
A. Yes.
Q. OK. Then he says, at the end, or towards the end, "I was told that management does not want anything in writing and that my emails would not be responded to in writing." Do you see this part? There you go. Do you see that?
A. Yes.
Q. "If that is still the case, I hope that my concerns can be addressed in another way," correct?
A. Yes.
Q. OK. So as of April 6, he's still telling somebody that somebody's not responding to him in writing, right?
A. Yes.

Q. OK. And then he says: "More than anything, I want this situation to go away. I feel like I'm being punished and that confidential information is told to Amol." Right?

A. Yes.

MS. SHROFF: OK. You can take that down.

Q. Now, on direct, you were asked questions about if this was the first time ever that somebody at your level of management had to be made or had to get involved in this level of dispute, correct?

A. If it was the first time I had been involved at my level in this type of dispute, yes, at that level.

Q. I just assume -- your tenure spanned a long time. Ten years or something, more than ten years?

A. As director of the center, my tenure spanned a year.

Q. All right. And you personally have never been involved with this level of a dispute, correct?

A. As director, no.

Q. And had there ever been a time that you can recall where somebody sought a protective order because their concerns were left unaddressed, at least according to them?

A. No.

Q. OK. Is it fair to say that it was upsetting that two CIA employees had gone to a public court to air this fight?

A. One employee chose to go to the court to air the fight. The other did not.

Q. One employee chose to go to court to air the fight. That's correct. Not something the CIA wanted, correct?
A. Not something that was typically done.
Q. I'm sorry. I apologize, but that really wasn't my question. My question was whether or not that was something that the CIA would want to see, ever.
A. I don't know that I can speak for the CIA.
Q. Well, you spoke for the CIA for a whole year, right?
A. I spoke for the Center for Cyber Intelligence --
Q. OK.
A. -- for a year.
Q. How about that? Let's try that. As the director of the CCI, it would not be something that you would want to see, ever, correct?
A. I would not want to see that, ever.
Q. Right. By the way, after Mr. Schulte went to court, were you aware that Amol also went to court to respond?
A. I think -- I don't recall that.
Q. Did Karen not brief you on this?
A. I can only speak to what I recall.
Q. So --
A. I don't recall that.
Q. -- you don't recall Karen briefing you on it then?
A. I don't recall it.
MS. SHROFF: May I just have a moment, your Honor?

THE COURT: Yes.

Q. You met with the government, did you not, to prepare for your testimony here?

A. I did.

Q. And you were actually kind enough to also speak to me, correct?

A. I did.

Q. Right. And the last time that you met with the government was on February 12. That was yesterday, correct?

A. Yes.

Q. OK. And who accompanied you to the meeting with Mr. Laroche? Who else was present, do you know?

A. I think Dave was present.

Q. Who's Dave?

THE COURT: Mr. Denton.

Q. Oh, Mr. Denton.

A. Yeah.

Q. Was anybody else also present?

A. There was an attorney there as well.

Q. What's the attorney's name?

A. Christine.

Q. And who does she work for?

A. She works for the CIA.

Q. So you had an attorney from the CIA present with you when the government was prepping you for testimony?

A. Yes.

MS. SHROFF: OK. I have nothing further.

MR. LAROCHE: No further questions, your Honor.

THE COURT: You're excused, Ms. Stith. Thank you very much.

THE WITNESS: Thank you.

THE COURT: Watch your step.

(Witness excused)

THE COURT: OK. As we've agreed before, we won't be sitting on Fridays. That's tomorrow, the 14th. It's Valentine's day. You're going to be off for Valentine's day. Monday is a national holiday, President's Day, so we won't be sitting on Monday either. You're going to have a long weekend, a four-day weekend, so remember my instructions. Don't talk about the case. Don't do any research. Don't listen to any radio or media concentrating on it. Keep an open mind.

We'll see you Tuesday morning at 9:00. Thank you very much.

(Continued on next page)

(Jury not present)

THE COURT: Please be seated.

Anything to take up?

MS. SHROFF: No, your Honor.

MR. LAROCHE: No, your Honor.

THE COURT: Mr. Zas, anything?

MR. ZAS: No, sir.

THE COURT: All right. See you on Tuesday morning.

MS. SHROFF: See you Tuesday.

MR. LAROCHE: Thank you, your Honor.

THE COURT: We have another matter.

(Adjourned to February 18, 2020, at 9:00 a.m.)

INDEX OF EXAMINATION

GOVERNMENT EXHIBITS

DEFENDANT EXHIBITS