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 5, 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 Fernando-Peiris
John Lee, Paralegals
Daniel Hartenstine
Daniella Medel, CISOs, Department of Justice

(In open court; jury not present)

THE COURT: Good morning. We're missing a couple of jurors.

MR. BRANDEN: We're missing a couple lawyers, too, but I thing they're just in the restroom and they'll be right here, Judge.

THE COURT: Okay. Thank you.

THE DEPUTY CLERK: Missing one still, Judge. Ms. Thompson.

THE COURT: Is Ms. Shroff here?

MR. ZAS: She is, Judge. She may have just stepped out to go to the ladies' room.

THE COURT: Do you want to take up the letter dated February 4 about the production of a binder? Can you talk about that, Mr. Zas?

MR. ZAS: Your Honor, I apologize. It is out of my realm of expertise.

THE COURT: Okay. We'll wait then.

Ms. Shroff, I want to talk about the letter you sent last night about 3506-04.

MS. SHROFF: Okay, I'm sorry, your Honor. I had to run back down to the SCIF. I apologize for keeping you waiting.

THE COURT: All right. I have the letter. I understand the letter. Mr. Laroche or somebody from the government, why can't you produce the binder?

MR. LAROCHE: May I just have one moment with Ms. Shroff. I just haven't seen the letter, I want to ask her what the letter is.

(Counsel conferring)

MR. LAROCHE: We're going to make the binder available, your Honor.

THE COURT: That takes care of that, Ms. Shroff. Anything else you want to take up?

MS. SHROFF: Nice to have that power, Judge.

THE COURT: 302 kind of dictates that you get the file, the binder as it was maintained at the time. Anything else to take up?

MR. ZAS: Your Honor, I did want to take something up with the Court, just on outstanding motions we don't think we've received a ruling on. There was a motion we made by letter dated January 17, it's the Smith v. Illinois issue about our inability to do any investigation of the CIA witnesses. And we moved for permission to conduct our usual background investigation on the witnesses, or alternatively --

THE COURT: I thought we took care of this at the final pretrial conference, Mr. Zas.

MR. ZAS: No, your Honor. I think at the final pretrial conference you asked the government to respond by letter, which they did. And that was the government's letter of January 24. We responded on January 27, and then we gave the Court a list of outstanding issues, including this one. So I just wanted to make sure we weren't waiving anything or the issue didn't get lost in the shuffle. It may have.

THE COURT: All right. We'll take a look. The dates of the -- give me the dates again.

MR. ZAS: The initial motion is a letter dated January 17, 2020. The issue is mentioned again in a letter of January 23. The government responded on January 24. We replied to that on January 27.

THE COURT: We didn't take it up at the pretrial conference? I have a vague recollection that you raised it before.

MR. ZAS: I raised it.

THE COURT: And the government consented to a Google search of the CIA witnesses.

MR. ZAS: That's right. We were advised that we had, we were permitted to conduct a Google search or similar Internet search of the witnesses' names, so long as we didn't specifically tie the name to the agency. We then objected to that, because we were then given guidance by Mr. Hartenstine that that meant we could not, for example, put the name in with important terms like WikiLeaks or spying or leaks or other items like that.

So, our problem is, as we sit here today with the first CIA witness about to testify, we've literally been able to do no investigation at all into this witness, or any of the 15 witnesses or so from the CIA. We're dependent entirely on what the government has given us. So I commend them for giving that to us but, we're supposed to have the right to do our own independent investigation.

THE COURT: I'll take a look. Thank you.

MR. ZAS: Thank you, sir.

THE COURT: Mr. Laroche, do you want the witness on the stand before the jury comes in?

MR. LAROCHE: That's fine, your Honor.

THE COURT: Okay. Do you want to bring in the witness. Is the next witness in the witness room?

MR. LAROCHE: Yes, your Honor.

THE COURT: The second witness today?

MR. LAROCHE: Not yet, your Honor. But this witness is going to be on for most, if not all, of the day.

THE COURT: Okay.

MR. LAROCHE: We will have that witness prepared to come up if it looks like he is going to finish.

THE COURT: Thank you.

(Jury present)

THE COURT: Before we start, let me confirm with the jury that all of you were successful in adhering to my instructions last night that you not discuss the matter, and you avoid any research or investigation. Okay. Remember, the case has to be decided based on the evidence that you hear in this courtroom and only this courtroom and only the evidence that you hear here.

Don't read any newspapers, don't watch any TV stories, don't do any independent research. Pay attention to what happens in the courtroom because that's what's going to define your task when you begin your deliberations. All right.

David.

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

THE WITNESS: Jeremy Weber.

(Witness sworn)

THE COURT: Please sit down. Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

JEREMY WEBER,

called as a witness by the Government,

having been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. LAROCHE:

Q. Good morning, Mr. Weber.

A. Good morning.

I don't have the sheet you had mentioned up here.

Q. Ah. Understood. We'll get you that sheet. Let's get started first.

Are you employed?

A. Yes, I am.

Q. Where do you work?

A. Central Intelligence Agency.

Q. How long have you worked at the Central Intelligence Agency?

A. Coming up on 10 years now.

Q. Does that also go by the CIA?

A. Yes, it does.

Q. What is the CIA?

A. The CIA is one of the executive agencies, we are tasked with collecting foreign intelligence.

Q. Prior to working at the CIA, where did you work?

A. I was active duty Marine Corps.

Q. How long were you in the Marines?

A. Almost six years.

Q. What were your roles in the Marines?

A. For the first half of my career in the Marine Corps, I was a data systems specialist, an IT guy. And then after that, I became a Marine security guard, guarding the embassies.

Q. I want to direct your attention to March 2017.

A. Yes.

Q. Were you employed by the CIA at that time?

A. Yes, I was.

Q. Are you familiar with a CIA group known as the Engineering

Development Group?

A. Yes, I am.

Q. In 2017, were you working in that group?

A. Yes, I was.

Q. Does the Engineering Development Group also go by EDG?

A. Yes, it does.

Q. Today I am going to refer to that as EDG or group.

A. Okay.

Q. Generally, speaking what did that group do?

A. The EDG was tasked with creating cyber capabilities for use in cyber operations.

Q. By cyber capabilities, did that include developing cyber tools?

A. Yes, that would be correct.

Q. What is a cyber tool?

A. Cyber tool would be anything from a script to a program that we created to collect information off of a computer network.

Q. You said that those tools were also used in operations; is that correct?

A. Yes, that's correct.

Q. What types of operations?

A. Cyber operations.

Q. Can you explain some of the targets of those operations, without identifying them specifically?

A. So, our targets typically fell into two categories. Foreign governments, or non-nation state actors.

Q. What do you mean by non-nation state actors?

A. Terrorists, typically.

Q. I want to direct your attention to March 7 of 2017.

A. Okay.

Q. Were you working that day?

A. Yes, I was.

Q. Were you working at the CIA that day?

A. Yes, I was.

Q. On that day, did you learn about the public disclosure of any of your group's work?

A. Yes, I did.

Q. Where was your group's work publicly disclosed?

A. It was disclosed on the internet, by WikiLeaks.

Q. Were there additional public disclosures of your group's work by WikiLeaks?

A. Yes, there was.

Q. Approximately how many?

A. I don't know the specific number. I think it was around 20 or so, plus or minus.

MR. LAROCHE: Your Honor, may I approach?

THE COURT: Yes, you may.

Q. Mr. Weber, I just handed you what's been entered into evidence as Government Exhibit 1. Do you recognize that?

A. Yes, I do.

Q. How do you recognize it?

A. After reviewing the exhibit, I made a mark on it that I would recognize.

Q. Does that exhibit contain the information that was disclosed by WikiLeaks from your group?

A. Yes, it does.

Q. Was the information disclosed by WikiLeaks from your group classified or unclassified?

A. It was mostly classified information.

Q. Where was that information stored within the group?

A. It was stored on our primary network called DevLAN.

Q. Is that a computer network?

A. Yes, it is.

Q. Is that computer network classified?

A. Yes, it is.

Q. Did everyone who worked in the group have access to all of the information contained on Government Exhibit 1?

A. No.

Q. I want you to look around the courtroom. Do you see anyone in the courtroom who worked in the group who had access to all of the information on Government Exhibit 1?

A. Yes.

Q. Can you please identify where that person is sitting.

A. He's sitting at the table there, looks like wearing a black jacket.

MR. LAROCHE: Your Honor, let the record reflect that the witness has identified the defendant.

THE COURT: Yes.

Q. How long have you known the defendant?

A. I knew him for the entirety of when I started at the agency, until his departure from the agency.

Q. While the defendant worked at the CIA, how often did you interact with him?

A. For most of the time, especially when he was a full-time officer, I would say daily.

Q. Can you describe what your relationship was like with him.

A. We were close. I would consider him a friend. We worked often together on projects. He was somebody that I looked to all the time to collaborate with. We were close over all.

Q. Did there come a time when your relationship changed?

A. Yes.

Q. When approximately did it change?

A. It would have been late 2015, early 2016. Josh became increasingly belligerent to another employee, and eventually I had had enough of the situation, and no longer considered him a friend.

Q. Are you aware of any time in which the defendant violated CIA policy using the classified computer network used by your group?

A. Yes.

Q. When approximately did that happen?

A. April 2016.

Q. How do you know it happened?

A. I witnessed the modification in some log files that showed that he modified some permissions, after explicitly being told otherwise on how they should be set.

Q. How did he modify those permissions?

A. Josh was an administrator of the system, and he used those administrative privileges to go against the orders of our leadership.

Q. Was he authorized to do that?

A. No, he was not.

Q. What, if any, steps did you take as a result of those actions?

A. I immediately informed management, and management had me come in, I believe the following day, with some other system administrators to remove his access to -- administrative access to the system.

Q. What are some of the reasons you took those steps?

A. The main reason was we no longer trusted him to be an administrator of the system. He had demonstrated that he was willing to do things other than what was explicitly told to him by his leadership.

Q. Why did you no longer trust him to be an administrator of the system?

A. The actions that he had taken to -- we had given him very specific instructions on how, how things were going to be. And the system was set up in such a way, following those instructions, Josh went and changed it to the way he wanted it to be, without informing anybody. And then, in addition to that, like I said, his interactions with the other employee and some statements he made about that employee were lies I felt.

Q. Did you view that as a problem?

A. Yes.

Q. Why?

A. The agency exists in a world of trust. We are granted access to classified information, and we are trusted to only use that information for the expressed reasons we're given access to it. If you can't trust the person that you're working with, you just aren't going to be able to do your daily job.

Q. Why is that a problem if you can't trust that person?

A. If you can't trust that person, you can't, you're not going to be able to work with them, because having access to some of this classified information could lead to grave damage to the U.S. government. If you can't share it with that person anymore, that's -- you're effectively worthless at the CIA.

Q. Now, you said that Government Exhibit 1 contains the group's work. Is that correct?

A. Yes.

Q. Did the leaks come from any particular part of your group's network?

A. Yes, it did.

Q. Which parts?

A. We had a product called Confluence, that was the data that was initially disclosed on the March 7. And then another product called Stash, later referred to as Bitbucket. It was renamed. That's where the data came for the second set.

Q. So let's start with Confluence. When was the Confluence information disclosed by WikiLeaks?

A. March 7.

Q. Approximately how much of Confluence was disclosed by WikiLeaks during that first leak?

MS. SHROFF: Objection, your Honor, as to personal knowledge from this witness on these issues.

THE COURT: Overruled.

Q. How much of Confluence was disclosed by WikiLeaks in the initial leak?

A. It appeared to be everything up to a certain date.

Q. You said that the subsequent leaks also had information from Stash?

A. That's correct.

Q. What types of things were disclosed from Stash?

A. The stuff that was disclosed from Stash was source code, user guides; things of that nature.

MR. LAROCHE: Ms. Hurst, can you please publish what's been entered into evidence as Government Exhibit 13.

Q. Do you see Government Exhibit 13 on the screen in front of you, Mr. Weber?

A. Yes, I do.

Q. Do you recognize this?

A. Yes, I do.

Q. What is it?

A. This is a user guide that we would often create to deliver with our tools.

MR. LAROCHE: Ms. Hurst, can you please zoom in on the top banner.

A. Yes.

Q. Mr. Weber, do you see that banner?

A. Yes, I do.

Q. Do you recognize it?

A. Yes, I do.

Q. What is it?

A. So this is a -- this is a banner that identifies both the classification of the document, as well as dissemination controls for said document.

Q. Which portion of this is the classification?

A. The first half.

Q. And that's the "secret;" is that correct?

A. Correct.

Q. And you said the other part has dissemination control?

A. That's correct.

Q. What do you mean by dissemination control?

A. So, in this scenario, "noforn" means no foreigners. This would -- this says who we could share the document with. You might have a scenario where this says "Rel To" and a country name. Which means we're willing to share this information with a specific country.

MR. LAROCHE: Could we zoom out again, Ms. Hurst.

Q. Mr. Weber, was this one of the Stash documents that was disclosed by WikiLeaks?

A. That is correct.

MR. LAROCHE: Could we, Ms. Hurst, can we please zoom in on the logo at the top.

Q. Do you recognize this logo?

A. Yes.

Q. What is it?

A. This is logo for the Information Operations Center.

Q. What is the Information Operations Center?

A. The Information Operations Center is a portion of the agency that's tasked with conducting cyber operations for the agency.

Q. I know you talked about the group which we've called EDG. Was EDG within that operations center?

A. Yes, it was.

MR. LAROCHE: Ms. Hurst, can you please zoom out. And zoom in on the title below the logo, please.

Q. Is this a reference to your group?

A. Yes, it is.

Q. You see the U next to it on the left?

MS. SHROFF: Your Honor, could we have a sidebar for a minute please?

THE COURT: What's the problem.

MS. SHROFF: I can't see my screen.

THE COURT: I'll see you at the sidebar.

(Continued on next page)

(At the sidebar)

THE COURT: What's the problem?

MS. SHROFF: I can't see my screen. Unbeknownst to me, behind my back, somebody's put a screen protector on it. I don't know why.

MR. LAROCHE: The government did not put a screen protector on it. We have no objection to removing the screen protector.

MS. SHROFF: Mr. Kamaraju's screen doesn't have a screen protector.

THE COURT: Listen, apparently it was put on there not on the government's intent. Do you want it off?

MS. SHROFF: I do want it off.

THE COURT: David, how long will it take to take the screen protector off?

THE DEPUTY CLERK: It takes seconds.

(Continued on next page)

(In open court)

THE COURT: Has the problem been corrected?

MS. SHROFF: Yes, it has.

THE COURT: Thank you. Mr. Laroche.

Q. The last question I asked was about the U on the left of this title here. What does that designate?

A. That's what we refer to as a portion mark. This sentence is a non-classified sentence. So the U is to help with identifying that.

Q. If we can just zoom out again. What is the top classification of this document?

A. Secret.

Q. How do you know that?

A. So, the classification banner at the top, we are told and we're trained that the classification contains the highest level of information that's within the document. So, in this case it would have been secret.

MR. LAROCHE: Ms. Hurst, can you please zoom in on lines that start Brutal Kangaroo and the next three lines below that.

Q. Are you familiar with Brutal Kangaroo?

A. Yes, I am.

Q. How are you familiar with it?

A. I advised Josh while he was writing it. I don't think I contributed anything of significance to this specific project.

But Brutal Kangaroo was also a successor to a tool that I had created.

Q. Is Brutal Kangaroo a cyber tool?

A. Yes, it is.

Q. Who developed Brutal Kangaroo?

A. Primarily Josh Schulte.

Q. Under Brutal Kangaroo there's Drifting Deadline?

A. Yes.

Q. What is Drifting Deadline?

A. Drifting Deadline was a specific component of the Brutal Kangaroo tool suite.

Q. What do you mean a component of the tool suite?

A. Brutal Kangaroo was meant to be a wide-ranging tool that would be used in multiple scenarios. So, it had different pieces to do different things on the network.

Q. And the bottom line of this says "user guide"?

A. Yes.

Q. What's a user guide?

A. A user guide is something developers would create so that our mission partners would know how to use the tool, what the risks of using the tool are, and things like that.

Q. You used the word mission partners. What do you mean by mission partners?

A. Mission partner is the official term for our customers. The people, we would make the tools and they would be used by another group. Those are our mission partners.

Q. Were those mission partners using the tools against foreign or domestic targets?

A. Foreign targets.

MR. LAROCHE: If we can zoom out again, please. Go to page four of this document.

Q. Do you recognize this page?

A. This appears to be page one still.

Q. Sorry. Page four of the PDF. Page one of the document. Do you recognize this page?

A. Yes.

MR. LAROCHE: Zoom in, Ms. Hurst, from scope -- perfect.

Q. Could you read the scope.

A. "This document establishes the user guide for Drifting Deadline version 1.2."

Q. And then also below 1.1, can you read the first sentence.

A. "Brutal Kangaroo is a tool suite for targeting closed networks by air gap jumping using thumb drives."

Q. Just what is that portion marking?

A. That is an S for secret.

Q. Why is it secret?

A. This is getting into the methods of how the tool works, which would have been considered secret.

Q. The first sentence refers to the tool suite that you referenced earlier; is that correct?

A. Yes.

Q. Then it says "targeting closed networks."

A. That's correct.

Q. What does that mean?

A. A closed network is a network that has limited connection to other networks. Typically, when we are referring to a closed network, we are saying a network that is not connected to the internet.

Q. Then next part says "targeting closed networks by air gap jumping." What does air gap jumping mean?

A. Air gap jumping was a trade craft term that we used. That referenced getting data off of a network without a network connection.

Q. Can you please read the second sentence.

A. "Brutal Kangaroo components create a custom covert network within the targeted closed network and provide functionality for executing surveys, directory listings, and arbitrary executables."

Q. Can you summarize what that's saying?

A. Brutal Kangaroo would -- created a custom file system on the thumb drives it was using to carry commands between machines on the network.

So in this specifically, they're talking about saying what type of computer surveys you would want, so this could be anything from what files are on a computer to what software is installed on the computer. Directory listings is one of those surveys I just talked about. And then arbitrary executables would be secondary payloads that we might deploy on the system.

Q. What do you mean by secondary payloads?

A. So, often this would be additional tools to do other things on the network, beyond just file collection.

Q. Give us an example.

A. Usually, the best example would be a back door, so that we would have future access to the system.

MR. LAROCHE: Ms. Hurst, can you please go to page six, and zoom in on the paragraph that starts the first tab to the bottom, the rest of the page.

Q. Mr. Weber, do you see that paragraph starting first tab?

A. Yes.

Q. Can you summarize what that's addressing.

A. So, these are the different execution vectors that Drifting Deadlines would use to gain execution, which that's, that is the official term for starting the program. So, sometimes the scenario would be a user would start the program for us, sometimes it would be what's referred to as an exploit to gain execution. The EZCheese link files and the Lachesis link files would be the exploits.

Q. Are you familiar with the term attribution?

A. Yes, I am.

Q. What does it mean?

A. Attribution is the identification of, it's tying an activity to an actor. In our scenario, it would be somebody catching CIA tools in the wild and then being able to say we know this is the CIA, because of these reasons. That's attribution.

Q. Is attribution to the CIA problematic for your work?

A. Yes, it is.

Q. Why?

A. So, we operate in secrecy. Foreign governments do not want us on their networks, and would complain, to put it lightly, if they caught us doing this. So, there is a wide gulf between having a tool caught, and then having information in there where a foreign government could publicly say the CIA was hacking us, the U.S. government is not being a good player.

Q. What, if any, impact did the disclosure of this have on attribution of this tool?

A. So --

MS. SHROFF: Objection.

THE COURT: Overruled.

A. These -- the information that is listed here would be clues to attribution. So if Brutal Kangaroo or Drifting Deadlines was caught on a foreign system somewhere, it might have been sitting on somebody's desk, they knew this would be malware. They wouldn't know necessarily whose malware it was. Seeing a document like this would allow them to start building a case against the U.S. government saying, no, this was -- this was a CIA tool that was used on our system.

Q. What, if any, impact would that attribution have on the use of these terms in the future?

A. If we were concerned about the attribution of a tool to the CIA, we would stop using it.

MR. LAROCHE: Ms. Hurst, you can pull that down.

Q. Mr. Weber, I just showed you one document that's contained on Government Exhibit 1. Is that correct?

A. Yes.

Q. Approximately how many documents were disclosed by WikiLeaks in Government Exhibit 1?

A. I don't know the exact number, but it would be thousands. More than hundreds. It took a team of -- I was on a team of about 10 people. It took us about a week of very long days to just go through the initial disclosure.

Q. Generally, what impact did the public disclosure of your group's information have on CIA's work?

A. It was crippling. We -- we were shut down for a significant amount of time. There was a significant amount of review about the operations that were ongoing to see what risk there was. And we had to recreate a significant number of capabilities.

Q. Why was there risk to operations?

A. It goes back to both the attribution piece as well as the information that was disclosed in WikiLeaks could be used by the defensive community to potentially identify and find out malware on foreign systems.

Q. What do you mean by malware?

A. Malware is the -- the industry term for cyber tools. I'm sorry.

Q. We're going to come back to the leak later. I want to switch gears just a little.

You said you started at the CIA, you've been at the CIA for about 10 years?

A. That's correct.

Q. Are you familiar with the phrase "security clearance"?

A. Yes.

Q. What is a security clearance?

A. Security clearance is the U.S. government's trust in us as individuals to have access to classified information.

Q. Do CIA employees need a security clearance to work there?

A. Yes, they do.

Q. Are there different levels of security clearance?

A. Yes, there are.

Q. What level?

A. There are three levels: Confidential, secret, and top secret.

Q. Can you describe some of the differences between those levels.

A. The difference in levels means the level of information that you would have access to, and it is graded by the amount of potential damage that could be done to the U.S. government. Confidential information, the official term is it would cause damage. Secret level, the official term is serious damage. And top secret is grave damage.

Q. What level security clearance do you need to work within the group?

A. Top secret.

Q. When did you first obtain your security clearance?

A. I first obtained a security clearance shortly after joining the Marine Corps.

Q. How do you obtain one?

A. At that time, it was a secret clearance, which involved me filling out a lot of paperwork that explained everything from where I've lived, who my friends were, who my family was, what my financial status was. So you would submit this paperwork, and then it's followed up by a background investigation where I would talk with an investigator essentially about the paperwork I had submitted.

Q. When you started at the agency, the CIA, did you obtain your top secret clearance?

A. I had obtained a top secret clearance prior to the CIA.

Q. When you started with the CIA, were you required to take an oath?

A. Yes, I was.

Q. Can you explain what oath you were required to take.

A. We take an oath to support and defend the Constitution of the United States.

Q. Where did you take that oath?

A. The oath is taken at the headquarters building of the CIA on the CIA's seal in the front lobby.

Q. Does that seal have any significance to the CIA?

A. That seal along with -- there's a memorial right next to the seal, it has a significant amount of significance. It's meant to represent everything that we are doing.

Q. Are all employees required to take that oath before they work at the CIA?

A. All staff employees.

Q. Let's talk for a moment about the structure of your group. The Engineering Development Group.

A. Okay.

MR. LAROCHE: Ms. Hurst, can you please publish to the witness, the parties and the Court what's marked as Government Exhibit 89.

Q. Do you see Government Exhibit 89 on your screen, Mr. Weber?

A. Yes, I do.

Q. What is it?

A. This is a portion of the org chart for CCI, the portion that EDG was.

Q. Does this exhibit fairly and accurately represent that portion of the org chart as it existed in 2015 and 2016?

A. Yes, it does.

MR. LAROCHE: The government would offer Government Exhibit 89 into evidence.

MS. SHROFF: No objection, your Honor.

THE COURT: 89 is in evidence.

(Government's Exhibit 89 received in evidence)

MR. LAROCHE: Ms. Hurst, can you please publish it for the jury.

Q. Mr. Weber, can we just start at the top. You referenced Center for Cyber Intelligence?

A. Yes.

Q. Where does that appear on this exhibit?

A. That's at the top here. CCI.

Q. What is CCI?

A. CCI -- I forget when exactly, it was a few years ago. We referenced IOC earlier. CCI was IOC renamed.

Q. IOC was the Information Operations Center; is that correct?

A. Yes.

Q. That was renamed as CCI?

A. That's correct.

Q. Below CCI there is a box for Engineering Development Group. Is that correct?

A. Yes.

Q. Is that the group you've been talking about today?

A. Yes.

Q. Below EDG, your group, what appears next?

A. Applied Engineering Division.

Q. Does that also go by AED?

A. Yes, it does.

Q. What is AED?

A. AED was a division in EDG. Our primary job was to create cyber tools for the group. We were in-house developers.

Q. What do you mean by in-house developers?

A. So, we worked in the same building that our mission partners worked in. The cyber operations are extremely tailored. It involves a lot of back and forth with our mission partners. So the in-house developers were closely tied into the operations so we can create the best capability possible.

Q. Below AED are five boxes. What do each those boxes reflect?

A. The different branches within AED.

Q. How many developers work within each of those branches?

A. Roughly, usually between 10 and 20 developers, depending on the branch.

Q. Focusing on the branch at the left, the Operations Support Branch. Are you familiar with that branch?

A. Yes.

Q. How are you familiar with it?

A. I spent approximately six years as a developer within OSB.

Q. Approximately what time frame?

A. From when I was hired all the way until 2016.

Q. Did the defendant also work in that branch?

A. Sorry, correction. It's 2017 is when I stopped working there.

And yes, the defendant did work in that branch.

Q. From approximately when?

A. The -- from the -- even before he was hired full-time, he was an intern in OSB. And then for almost the entirety of his career he was in OSB.

Q. What was the purpose of that branch, OSB?

A. OSB was focused on what we referred to as physical access operations.

Q. What is that?

A. Physical access operation is a scenario where we, the agency, had the capability to effectively touch a computer, be it through an agency officer or an agency asset.

Q. What do you mean by touch a computer?

A. It could be anything. It could be somebody who was willing to type on a keyboard for us. It often was somebody who was willing to plug a thumb drive into the machine. Or it could be a scenario where somebody was willing to literally pick a machine up and walk off with it.

Q. You used the word "asset" a second ago.

A. Yes.

Q. What were you referring to?

A. An asset is a term in the CIA for a -- for a foreigner who has been recruited to work for the CIA.

Q. What was the culture of OSB like when you worked there?

A. We were very mission focused. We, we work closely with each other. We got along with each other. We were, I would say, mostly friends. It was, the -- working at the agency, you always kind of have the finish line in your sights and the exact mission that you're working on, and that's what drives us.

Q. What do you mean by mission?

A. So, our mission is to, again, it's to support and defend the Constitution. So, we are tasked with getting information to policy makers so that they can effectively chart the direction the United States should go.

Q. Did OSB have a professional atmosphere while you were there?

A. It was mostly professional. I would say no more or less professional than any other software development shop.

Q. What do you mean by that?

A. You know, again, our primary focus was on the mission. But, you know, we had fun at work, too. We would occasionally poke fun at each other. We were all friends.

Q. How often did you interact with the defendant while he was in the branch?

A. I would say daily.

Q. Generally, what were those interactions like?

A. I, I considered him a friend. Again, I worked closely with him. I liked working with him. Josh, you know, I would say mostly positive, although Josh, Josh sometimes would exhaust you a little bit in those interactions.

Q. What do you mean by that?

A. You know, Josh was very opinionated on the way things should be done. And wasn't somebody that could often be swayed of said opinion. So, he had some rough edges that you would have to deal with. You kind of took the good with the bad.

Q. Did you observe the defendant interact with other developers in the branch?

A. Yes.

Q. What were those interactions like?

A. Mostly positive outside of one developer. I think most developers within the branch would have the same opinion.

MS. SHROFF: Objection as to what opinion anyone else had.

THE COURT: Yes. Sustained.

Q. You said one, as to one developer there was a different relationship; is that correct?

A. Yes.

Q. What was that developer's name?

A. Amol.

Q. We'll come back to Amol and the defendant later.

Looking back at the chart that's in front of you.

A. Okay.

Q. The top of the chart has CCI; is that correct?

A. That's correct.

Q. While you worked within CCI, where was it physically located?

A. CCI was in an office building that was west of Washington, D.C.

Q. Just going to refer to that as the CCI building or the office. Okay?

A. Okay.

Q. Was anyone free to walk into that office?

A. No.

Q. What stopped them?

A. There was a fence around the entire compound, and to get past that fence and enter the compound, you had to get past armed security.

Q. How was that security armed?

A. Military grade weapons.

Q. How did you get past that security?

A. To get past that security, you had to present your identification. For full-time employees, that would be your

I.C. badge, and then they would let you on to the compound.

Q. You said I.C. badge. What's the I.C. stand for?

A. Intelligence community.

Q. Is the CIA part of the intelligence community?

A. Yes, it is.

Q. Once you got through the armed guards, could you just walk into the office building?

A. No.

Q. What stopped you?

A. There were -- the way I would typically go in, were what we referred to as full-height turnstiles. To get past those, you would need to, you would need to badge in, which would be, you would tap your badge against like a receiver. And then you would have to put in a private code. The other way that you could go in were also turnstiles that had armed security by them.

Q. Could you hop over those turnstiles?

A. The ones with the armed security, you could hop over, I would not recommend it. The turnstiles that I typically went through there was no way to hop over. It was essentially a wall.

Q. Did the CIA store classified information at this office?

A. Yes, it did.

Q. Generally speaking, in what kinds of places did it store that classified information?

A. What we referred to as a SCIF. A secure compartmented information facility. It is, it is a large vault.

Q. What do you mean by that?

A. So, SCIFs have very strict rules on how they are set up, access controls, things like that. They have heavy metal doors that the first person that comes in for day has to put in a combination to unlock the door. And then anybody after that would have to badge in to gain access to the room.

Q. Were there any restrictions on what you could bring into that office building?

A. Yes, significant.

Q. What types of restrictions?

A. There's, pretty much any personal electronics were not allowed. Weapons, photography equipment, cell phones. When you come into any agency building, there's always a sign that says these are the prohibited items. It is a pretty lengthy sign.

Q. Why are you not permitted to bring electronic devices into the office?

A. They would introduce a risk to the classified information that's stored there.

Q. What do you mean by that?

A. The best example would be if you brought in a cell phone. You, an adversary might be able to leverage that cell phone to listen to conversations that were ongoing in there. Or something like that.

Q. When you badged into the building through the turnstiles, were you in a SCIF?

A. No.

Q. Where were the SCIFs located within the building?

A. They -- they were all -- they were all individual rooms that you had to enter after badging through.

MR. LAROCHE: Your Honor, with the Court's permission, I'd like to read a stipulation.

THE COURT: Yes.

MR. LAROCHE: It is hereby stipulated and agreed by and among the United States of America by Geoffrey S. Berman, United States Attorney for the Southern District of New York, David W. Denton, Jr., Sidhardha Kamaraju, and Matthew Laroche, Assistant United States Attorneys, of counsel, and Joshua Adam Schulte, the defendant, by and with the consent of his counsel, Sabrina Shroff, Esq,. Edward Zas, Esq., and James Branden, Esq., that:

Government Exhibit 100 is a compact disc containing true and accurate CIA badge records for (i) Joshua Adam Schulte identified as Government Exhibits 105, 107, 108 and 109; (ii) Rufus, identified as Government Exhibits 101 and 112; (iii) David, identified as Government Exhibits 102 and 113; (iv) Timothy identified as Government Exhibits 103 and 114; (v) Andrew identified as Government Exhibit 104; (vi) Jeremy Weber identified as Government Exhibits 106 and 117; (vii) Michael identified as Government Exhibit 115; and (viii) Amol identified as Government Exhibit 116. Government Exhibits 101 through 109 and 112 through 117 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 the regularly conducted business activity; and it was the regular practice of that business activity to maintain the records. The time stamps on Government Exhibits 101 through 109 and 112 through 117 reflect local time in 24-hour format.

Government Exhibit 111 is a true and accurate copy of floor plans for the eighth and ninth floor for the CIA's Center for Cyber Intelligence office in which the defendant worked.

Government Exhibit 200 is a compact disc containing true and correct copies of portions of the defendant's CIA personnel file, including Government Exhibit 201, which is a training the defendant took while employed at the CIA; Government Exhibit 202, which is a portion of the defendant's CIA employee bio; government Exhibits 401 through 405, which is various non-disclosure agreements and security paperwork signed by the defendant prior to resigning from the CIA; Government Exhibits 406 and 408, which are various of the defendant's performance activity reports at the CIA; Government Exhibit 409 is a letter of warning provided to the defendant on or about June 22, 2016; and Government Exhibit 411 is a complaint filed by the defendant to the Office of Equal Employment Opportunity Commission.

Government Exhibit 300 is a compact disc containing true and accurate copies of documents marked as Government Exhibits 301 through 304, recovered from the defendant's desk area following his resignation from the CIA.

Government Exhibit 500 is a compact disc containing true and correct copies of portions of the defendant's CIA security file, including Government Exhibits 506 through 507, which are outside activities reports completed by the defendant while employed at the CIA; Government Exhibit 505, which is a complainant statement signed by the defendant while employed at the CIA; Government Exhibit 508 is excerpts of a recording of an April 8, 2016, interview of the defendant while at the CIA; and Government Exhibit 509 is excerpts of a recording of a July 19, 2016 interview of the defendant while at the CIA.

Government Exhibits 601 through 616 are true and accurate copies of network documentation for certain CIA computer systems.

Government Exhibits 701, 702, 704 through 708, 712 through 714, 716, 718, 719 and 720 are true and accurate copies of electronic communications that were transmitted over CIA messaging systems. The time stamps on the foregoing exhibits reflect local time in 24-hour format.

And Government Exhibits 1001 through 1012, 1015 through 1056, 1058 through 1098, 1100 through 1103, 1105, 1107, 1108, 1110 through 1116, 1118, 19, 21, 24, 1128 through 1130000 are true and accurate copies of e-mail communications sent and received using CIA computer systems.

And finally, Government Exhibit 5001 is a true and accurate copy of portions of the CIA's October 17, 2017 WikiLeaks Task Force Final Report.

It is further stipulated and agreed that this stipulation, Government Exhibit 3004, and all of the exhibits identified in this stipulation, may be received in evidence as government exhibits at trial.

THE COURT: They're received in evidence.

MR. LAROCHE: Thank you, your Honor.

(Government's Exhibit 3004, 100, 111, 200, 300, 500 received in evidence)

(Government's Exhibit 601-616, 701, 702, 704-708 received in evidence)

(Government's Exhibit 712-714, 716, 718, 719, 720 received in evidence)

(Government's Exhibit 1001-1012, 1015-1056, 1058-1098 received in evidence)

(Government's Exhibit 1100-1103, 1105, 1107, 1108 received in evidence)

(Government's Exhibit 1110-1116, 1118, 1119, 1121 received in evidence)

(Government's Exhibit 1124, 1128-1130, 1132-1137, 5001 received in evidence)

MR. LAROCHE: Ms. Hurst, can you please publish what's marked as Government Exhibit 1011. Sorry. 111. And go to the second page of this exhibit.

Q. Mr. Weber, do you recognize this?

A. Yes, I do.

Q. What is this?

A. This is a floor plan for the ninth floor of our office building.

Q. Just to orient us a bit, was OSB located on the ninth floor as of 2015 and 2016?

A. Yes, it was.

MR. LAROCHE: Ms. Hurst, can you just zoom in on the middle portion of this. Right in the middle of the document.

Q. Just in the middle there, Mr. Weber, what are we looking at?

A. The middle is the elevators to get to the ninth floor.

Q. Can you just circle on the screen where the elevators are.

A. So this was the primary bank of elevators. And then this one over here is a freight elevator.

Q. The portions you just circled, is that within a SCIF area?

A. No, it is not.

Q. We can zoom back out, please.

MS. SHROFF: Mr. Laroche, are we looking at the circling?

MR. BRANDEN: The circle is not showing up.

THE DEPUTY CLERK: Mr. Laroche, I think now it's working.

MR. LAROCHE: Thank you, David.

Q. If we could clear the screen, please.

THE COURT: The yellow circle is the elevators and the purple circle is the freight elevators?

THE WITNESS: I don't know where the yellow line came from, your Honor. The larger circle is the regular elevators. And actually, the circles that were just shown were off.

MR. LAROCHE: Maybe we could zoom in again so we can have the record clear for everyone.

Q. Can you please just circle, once this is zoomed in, the elevators again, please. Thank you.

A. Yes. So, these are the regular use elevators, and then this right here is a freight elevator.

MR. LAROCHE: If we can zoom out again, please.

Q. Mr. Weber, can you please circle where OSB sat as of 2015 and 2016.

A. Yes. That would be this area right over here.

MR. LAROCHE: Can we zoom in on that area, please, Ms. Hurst.

Q. Can you circle that area again where OSB sat.

A. Yes. This area.

Q. I think OSB appears on this zoomed in version. Could you just circle it?

A. Yes.

Q. What do these reflect? I know they're a little blurry.

A. The area that I circled would have been cubicles.

Q. Is this area within a SCIF?

A. Yes, it is.

Q. How do you get into this SCIF?

A. There were multiple entrances to this SCIF, but it was all through, again, you would badge into the SCIF through one of the many doors.

Q. As of 2015, can you circle where you sat within OSB?

A. Yes.

Q. What about the defendant?

MR. LAROCHE: Thank you. We can pull that exhibit down.

Q. We've been talking about the office that CCI worked in.

A. Yes.

Q. Were you allowed take classified information out of that building?

A. Only with specific authorization.

Q. How would you obtain that authorization?

A. You would request it. There was a form you would, or like a web page you would go to, to say what you were taking, where you were taking it to, and what the purpose was for traveling with classified information.

Q. Were you allowed to take classified information home?

A. No.

Q. Why not?

A. Your home is not a secure place to store classified information.

Q. Was there any procedure in place if you did take classified information to a place you weren't supposed to?

A. Yes, there was.

Q. Can you describe that procedure.

A. If you mistakenly took classified information to a location you weren't supposed to, you were instructed to immediately return to whatever closest facility there was, and then report to both the agency security officer as well as your leadership.

Q. Did you ever have to follow that procedure?

A. Yes, I did.

Q. Can you explain what happened?

A. So, early in my career, it was tax time. We are, we are sent our tax documents electronically. I printed off the tax documents which are unclassified, but, whenever you print something, you have what is referred to as a cover page. And that cover page says treat this information as classified. I accidently brought that cover page home one day.

Q. Can you describe what that cover page looks like?

A. It just has your user name and says the information following this might contain classified information. And that it was U.S. government.

Q. What did you do with the cover page after you found it at home?

A. Brought it back into work.

Q. What happened as a result of that?

A. I reported it to management and the ASO, but there was no further action. They told me not to do it again.

Q. Did you use a classified e-mail system at the CIA?

A. Yes, I did.

Q. Did you ever send unclassified e-mails on that system?

A. Yes, I did.

Q. Why would you do that?

A. The -- the classification of an e-mail has nothing to do with the system that it's on. It is the information that's contained in that e-mail. So, an unclassified e-mail might be something as simple as, let's meet at, you know, 3 p.m. in this room number. Nothing in there is damaging to the U.S. government. That would be an unclassified e-mail.

Q. How would you notify someone if you were sending an unclassified e-mail?

A. Every single e-mail that we sent, you were required to classify before sending it. So, the e-mail would carry a classification banner as well as a classification block.

Q. Just want to show you one example.

MR. LAROCHE: Ms. Hurst, if we can publish Government Exhibit 1023. If we can go to the second page of this exhibit. Just zoom in on the to from line here.

Q. Do you recognize this to be a CIA e-mail?

A. Yes, I do.

Q. Who sent this e-mail?

A. This would have been sent by Joshua Schulte.

Q. When did he send it?

A. January 6, 2016, at 3:06 p.m.

Q. Who did he send it to?

A. Rufus.

Q. Did he copy anyone on the e-mail?

A. He copied myself and Sean.

Q. What was the subject of this e-mail?

A. "Migration of Atlassian servers and support back to ISB."

MR. LAROCHE: If we can zoom from classification down.

Q. Just starting at the top of the screen, there is a classification secret/noforn with a cross through. What does that reflect?

A. So, this would have been the overall classification of the e-mail.

Q. Who classified the e-mail?

A. The e-mail is classified by the sender, so in this case Josh.

Q. How would the sender classify the e-mail?

A. There was a tool tied into our e-mail system that you would select what the classification was, as well as what reason you were classifying the document.

Q. Okay. We'll come back to the substance of this e-mail later.

MR. LAROCHE: Ms. Hurst, you can pull that down. Thank you.

Q. You stated and you talked a little bit about the development of cyber tools by the group.

A. Yes.

Q. Generally speaking -- strike that.

Who tasked you to create cyber tools?

A. Our mission partners would.

Q. Who were your mission partners?

A. In -- typically, it's COG, which was another group within CCI. Like I mentioned earlier, EDG made the tools, COG would deploy them in operations.

Q. What does COG stand for?

A. Computer Operations Group.

Q. After you were tasked to create a cyber tool, how would you go about creating it?

A. So, there was significant back and forth when you are creating a tool. You would interact closely with COG to make sure you were creating the right thing. Once you understood the mission parameters, the AED, we would write the source code that would eventually in turn create the capability.

Q. You used the term "source code."

A. Yes.

Q. What is source code?

A. So, source code is what software developers create. It is human readable computer instructions that eventually will be compiled into a computer readable program.

Q. How did you go about developing source code?

A. We would write it. This is what we're trained to do.

Q. Are you familiar with a cyber tool called Marble or Marbler?

A. Yes, I am.

Q. Generally speaking, what does that tool do?

A. It was an internal tool, meant -- it was used by developers in AED to aid in the development of capabilities. Its job was to, one of our pieces of trade craft was to obfuscate strings which could be identifying information in a binary. So, Marbler would obfuscate the strings for us.

Q. You used the term "trade craft." What does that mean?

A. Trade craft is the lessons learned, the rules, everything like -- you're taught how to be a software developer in college. The agency then takes that raw material and trains you on how to be somebody who creates cyber tools. The trade craft is the training that you get for this is how you, you know, do X, Y and Z. These are best practices, things like that.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 12-2.

Q. Mr. Weber, do you recognize this?

A. Yes, I do.

Q. What is it?

A. This is source code.

Q. Was this source code disclosed by WikiLeaks?

A. Yes, it was.

Q. What is this source code for?

A. This was a portion of Marbler.

Q. How do you recognize this to be source code?

A. I wrote stuff very similar to this. This is C++ code which is a computer language. And a lot of the words and things in here are what are referred to as key words. So, anybody who is a C++ developer would recognize this.

Q. So I want to go to one page of this and see if you can help us understand it. If we go to page five. Then if we can just zoom in on the top all the way down to "go to reset." That's fine. Just want to focus you on the middle where it starts "generate modified files."

Do you see that?

A. Yes.

Q. Could you summarize what that's saying.

A. So, this is generate modified files is a function call.

So, this is the -- what's done in generate modified files is defined elsewhere in the source. But, this function is called, and then immediately after this function, we check to see if there was any error during the running of this. And if there was an error, we print to the user that there was a problem and that you're resetting the files before proceeding on.

Q. What do you mean by print to the user?

A. So, Marbler was what we referred to as a command line tool. Think your old DOS prompt where you've got just text on the screen. So, this would, this would write to that screen error in modifying files resetting to original files.

Q. Is this source code classified?

A. Yes, it is.

Q. Why?

A. The techniques in here are part of our trade craft. And having access to this information and the tie to the CIA would help an adversary with the attribution aspect of the identification.

MR. LAROCHE: Ms. Hurst, we can pull that down.

Q. When source code is complete for a tool that you're developing, what happens to it?

A. It's, in the case of C++, it's compiled, which is a tool that is used to convert that human readable files into machine readable code.

Q. What is that machine readable code then called?

A. We typically refer to that as a binary or a program.

Q. Why do you create binary from the source code?

A. So, in compiled languages, computers can't execute source code. So, it doesn't understand, it doesn't understand the documents that we write, so it's converted to a language the computer understands.

Q. Other than the source code and the binary, do developers create any documentation for their cyber tools?

A. Yes.

Q. What are some of the types of documentation they create?

A. The main type of documentation you would see would be a user guide, which explains how to use the tool, why you would use the tool, and what scenarios you would use the tool. We also were a bureaucracy at heart, so there would also be delivery records with everything that we did and there would be a paper trail. We would help in the creation of those documents as well.

Q. When the source code, the binary and those documents are complete, what happens to the tool?

A. We, it would go through what we referred to as the delivery process. That information would be handed over to our SIs, system integrators, who would then take it to the configuration management team who would store the information, as well as hand it over to COG so that they could use the tool.

Q. Earlier in your testimony you talked about a computer network that was used by the group; is that correct?

A. Yes.

Q. From which the information on Government Exhibit 1 came from. Is that right?

A. Yes.

Q. I want to focus you on 2015 and 2016.

A. Okay.

Q. Was that computer network used to develop cyber tools?

A. Yes, it was.

Q. What was that computer network called?

A. DevLAN.

Q. What does DevLAN mean?

A. It was, it was abbreviation for dev, which short for development, and LAN was short for local area network. So, it was just a shortened term to reference that.

Q. What's local area network mean?

A. Local area network is an industry term for a network that is controlled by a company or something like that.

Q. Were you familiar with the DevLAN network?

A. Portions of it.

Q. How did you become familiar with portions of that network?

A. One, my day-to-day job was leveraging the resources that were on DevLAN. And secondly, I was an administrator for a portion of the network.

Q. What do you mean by administrator?

A. I had additional privileges on some of the services that were run on the network, to ensure that those services stayed up and running, granting access to who needed access to those services, things like that.

Q. Did any other developers share in those administrative privileges?

A. Yes.

Q. Who?

A. At the time you referenced, it would have been Joshua Schulte. Just before that, it would have been Patrick.

Q. Who is Patrick?

A. Patrick was a developer within AED as well. He originally brought the Atlassian products in house and helped set them up. But he was selected for a new assignment, and passed those responsibilities off to me.

Q. What was the classification level of the DevLAN network?

A. Top secret.

Q. Why did it have that classification level?

A. The information that was on the network would often be up to top secret in nature.

Q. Was DevLAN connected to any unclassified network?

A. No, it was not.

Q. Was DevLAN connected to the internet?

A. No, it was not.

Q. Why not?

A. Being connected to the internet would pose a serious risk to the security of that network. It would give essentially the adversaries a front door into accessing it.

Q. I'd like to focus on how the DevLAN network was set up or its infrastructure. Generally speaking, what is network infrastructure?

A. Network infrastructure is anything that's needed for a computer network to run. Generally speaking, you've got three categories of stuff. The end user's machines, think the laptop or desktop that you would use on a daily basis. The servers, which are powerful machines that sit in the back that contain a lot of the information. And then intermediary devices on the network whose job is to transfer the data back and forth.

Q. Are you familiar with the term "closed network"?

A. Yes, I am.

Q. What is a closed network?

A. A closed network is a network that has limited access, if any access to other networks. And traditionally speaking, when we refer to a closed network, we are saying it is a network that is not connected to the internet.

Q. Was DevLAN a closed network?

A. Yes, it was.

Q. Why was it a closed network?

A. It was a top secret network, which meant that there were, there was a lot of security procedures that we had to follow.

And one of the easier ways to defend a network is by making sure that it does not have access to the internet.

MR. LAROCHE: Ms. Hurst, can you please publish to the Court, the parties, and the witness what's marked as Government Exhibit 1251.

Q. Mr. Weber, do you recognize this?

A. Yes, I do.

Q. What is it?

A. It is a high level, it is a high-level view of portions of DevLAN, as well as COG's network and Hickok.

Q. Does it fairly and accurately represent those portions of the network you just described and in about 2015 and 2016?

A. Yes, it does.

MR. LAROCHE: The government offers 1251 into evidence.

MS. SHROFF: Your Honor, we have an objection.

THE COURT: You have no objection?

MS. SHROFF: We do have an objection.

THE COURT: It's overruled.

MR. LAROCHE: Can we publish that for the jury?

THE COURT: 1251 is received in evidence.

(Government's Exhibit 1251 received in evidence)

MR. LAROCHE: Thank you, your Honor.

Q. There is a lot on this screen. We're going to walk through it, Mr. Weber. First, did DevLAN run computer software?

A. Yes, it did.

Q. Are you familiar with the term Atlassian?

A. Yes, I am.

Q. What is Atlassian?

A. Atlassian is a commercial company that creates products for software development.

Q. Did DevLAN include certain Atlassian services?

A. Yes, it did.

Q. What services?

A. There were five of them: Confluence, Bamboo, Crowd, Jira, and at the time, it was called Stash, that product has been now renamed to Bitbucket.

Q. If we can focus on the top left. You see some of the Atlassian services here?

A. Yes.

Q. Can we circle Confluence, please. What is Confluence?

A. Confluence is a product for generating or presenting user-generated content. It's similar to something like Wikipedia where multiple users can edit the same page, and it's a collaborative work environment.

Q. Can you please circle Bamboo on the screen. This is another one of the Atlassian services run on DevLAN?

A. Yes, it is.

Q. What did Bamboo do?

A. Bamboo, to use an industry term, was used for continuous integration. Which meant whenever source code was changed, Bamboo would detect that change, compile the code, and test the code. It was meant to make it so that if you introduced an error in your code, you discovered it early and can correct it right away.

MR. LAROCHE: Ms. Hurst, if you can zoom out, please. Then zoom in on the box with the Stash server.

Q. Can you please circle Stash on this. What was Stash?

A. Stash was meant to, to back up the source code that we wrote on a daily basis, as well as provide an area for us to collaborate and discuss that source code.

Q. Can you please circle Crowd. What did Crowd do?

A. Crowd's job was to translate the user permissions that were -- like the user authentication was handled by an external service called Active Directory. So, all of the user authentication, things like that, would be handled by Active Directory. Crowd's job was to interface with Active Directory and then let the Atlassian products know who an authorized user was and what groups they belonged to.

MR. LAROCHE: Just zoom out one more time, please. Zoom in on the box with Hickok.

Q. What is Jira?

A. Jira is a tool for issue tracking. Which, that's everything that we need to do when we are developing a tool. It could be anything from the background of this web page needs to be blue and not green, to something like in this scenario, the program crashes, and we need to fix this. Jira was meant to track all of those work items. So that you can report the status of how far you've progressed in your development.

Q. If we can zoom out again, please. Did DevLAN also have hardware?

A. Yes, it did.

Q. What types of hardware did it have?

A. It had, all, all types of hardware. For the most part, the users had desktops as their work machines. It had computer servers. It had switches, routers, everything that you would find on a traditional network.

Q. Let's focus on the servers.

MR. LAROCHE: Ms. Hurst, if you can zoom in on the top left, the ESXi server.

Q. What is an ESXi server?

A. ESXi is another commercial tool that its job is to -- it's referred to as a hypervisor. It's meant to enable running what we refer to as virtual machines. It allows you to run multiple virtual machines on a single set of hardware. Something like that.

Q. In 2015, what branch did the ESXi server belong to?

A. This specific one belonged to OSB.

Q. What programs were being run on that ESXi server?

A. It was running a Confluence virtual machine, a Bamboo virtual machine, as well as a collection of development VMs for different purposes.

Q. You used the term "virtual machine."

A. Yes.

Q. Is that the same thing as a VM?

A. Yes.

Q. What is a virtual machine?

A. A virtual machine is technology that we use in the IT world. It is a way to try and separate the operating system and any services from the hardware it's running on.

Hardware ages and eventually fails. So, virtual machines are supposed to make it so that you're agnostic to the hardware you're running on. So when a server begins to fail, you can quickly migrate that service to something new.

Q. What's the purpose of that?

A. It's, in the IT world, you are pretty much judged based solely on what we refer to as uptime, meaning, is a user able to use the service that you're responsible for. So, having a server fail would cause significant impact on your uptime. And this is a way of just making sure that that wouldn't happen.

MR. LAROCHE: Ms. Hurst, can you please zoom out then zoom in on the Stash server.

Q. Was there a separate server that was running Stash?

A. That's correct.

Q. Can you explain that?

A. Stash, the server was owned and operated by ISB. Stash was not a virtual machine, because there is a cost to running virtual machines. It's not as efficient as running on a straight hardware. And we wanted to make sure Stash, which was the most used of the services, had enough power to, you know, meet the division's needs.

Q. You used the term ISB.

A. Yes.

Q. What is ISB?

A. ISB was the branch within EDG whose focus was on system administration of DevLAN.

Q. What does ISB stand for?

A. Infrastructure Support Branch.

MR. LAROCHE: Ms. Hurst, can you please zoom out. Can we please publish again Government Exhibit 111.

Q. You just talked about the OSB's ESXi server. Is that correct?

A. Yes.

Q. And a Stash server?

A. Yes.

Q. Where were those located?

A. They were located in server rooms.

Q. On what floor?

A. The ninth floor.

Q. Let's start with the OSB ESXi server.

A. Okay.

Q. Do you see the server room in which the OSB ESXi server was located as of 2015 and 2016?

A. Yes, I do.

Q. Can you please circle that server room.

A. This one right here.

Q. Is that server room within a vault?

A. Yes, it is.

Q. Can you please circle the server room in which the Stash server was located in 2015 and 2016.

A. That would be this one right here.

Q. Who did that server room belong to?

A. ISB.

Q. Thank you.

MR. LAROCHE: We can take that down, please.

Q. You stated that COG, the Computer Operations Group, used the tools that were developed by some of the branches within EDG; is that right?

A. That's correct.

Q. Did COG users have their own computer network?

A. Yes, they did.

Q. I am going to refer to as the COG network.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1251 again.

Q. Did COG users have access to the cyber tools on DevLAN?

A. Not directly, no.

Q. What do you mean by that?

A. Any tools that we created on DevLAN would be delivered to COG, usually by CD, and then stored on COG's network.

Q. Did COG users have access to Confluence on DevLAN?

A. No, they did not.

Q. Did COG users have access to any of the Atlassian services?

A. Yes, they did.

Q. Which one?

A. Jira.

Q. How did COG users have access to Jira?

A. Jira existed on an intermediary network in between DevLAN and COG called Hickok.

Q. Could COG users access other Atlassian services through Hickok?

A. No.

Q. How do you know that?

A. COG users did not have credentials to DevLAN. And all of the other Atlassian products would require DevLAN credentials. And also, COG users, there wasn't a network, direct network connection that they could travel over.

MR. LAROCHE: We can pull that down for a second, Ms. Hurst.

Q. Let's talk for a moment about how the Atlassian services were backed up.

A. Okay.

Q. Are you familiar with the term "data backup"?

A. Yes, I am.

Q. What does that mean?

A. So, the data we created on DevLAN was our day-to-day work. Losing that would mean that we would have to recreate it and would take a significant amount of time.

To defend against this, you would create a data backup, which was a copy of the data done usually daily or something of that frequency. So that if there was an incident, disaster, something like that, we could get back without losing much work.

Q. Focusing on 2015, were the Atlassian services backed up?

A. Yes, they were.

Q. How?

A. So, in 2015, the data backups were to the -- originally to the local drives that they were -- the local machines that they existed on. So Confluence wrote to the Confluence machine, Stash back up its data to the Stash machine.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1251 again. Just zoom in on the ESXi server for a moment.

Q. Can you explain what you mean by there being a time where the backups were stored on the machines themselves?

A. Yes. So, in this case, Confluence, all of the data that was generated, was on Confluence VM. So on a hard drive that belonged to Confluence. The backups would write to the same hard drive, just a different folder location.

Q. Was that problematic?

A. Very.

Q. Why?

A. Two reasons. One, the backups took up a significant amount of space. And it caused a problems with Stash, where one day Stash would no longer turn on, because we literally used up every, every bit of hard drive space for that machine.

But more importantly, a backup to the local machine is just a bad idea. Because most likely, your reason for needing a backup is the computer that the service was running on failed. And so your backup failed in that scenario too.

Q. Did there come a time when the backups were not stored locally?

A. Yes.

Q. Where were they stored after that?

A. They were stored on a NetApp on DevLAN. And then to an offsite location as well.

MR. LAROCHE: Ms. Hurst, can you zoom out for a second. Then zoom in on the middle bottom box, the NetApp server.

Q. Is this the NetApp you were referring to?

A. Yes.

Q. What is a NetApp server, generally?

A. NetApp is another commercial technology. They are focused on what is referred to as network attached storage, which is meant to be file systems that are accessed over a network drive.

(Continued on next page)

BY MR. LAROCHE:

Q. Where were the backups stored on NetApp?

A. There was a folder created on the NetApp called Altabackup.

Q. How often were the Atlassian services backed up to the Altabackup?

A. I believe it was daily.

Q. How were the data backups moved to the Altabackup from the Atlassian services?

A. So, when Altabackup was created, each of the Atlassian products was modified as well as the VMs or machines they were running on. The Altabackup folder was what we refer to as mounted in the Linux drive, so for general purposes, that meant -- it looked like any other folder on your system.

Q. Were the backups stored within any other location other than the Altabackup?

A. Yes.

Q. Where?

A. They were in an offsite location also in the WMA area.

Q. Other than the Alta backups, was there anything else stored on the NetApp server?

A. Yes, there was.

Q. What else was stored on the NetApp server?

A. A significant amount of information. Some examples would be users' home directories, which, for every DevLAN user, they would get a folder on the NetApp that they controlled who had access to what on that folder. And then there was also just a general file share, so if we had software that we had downloaded or something like that, it could be stored there.

Q. Are you familiar with the term Gold source copies?

A. Yes, I am.

Q. What are those?

A. When we would finish a tool and deliver it to COG, there would be an official record made. So the final version of the binary that we were delivering, any documentation and any source code would be given to the configuration management team, and that information would then be stored as an official record.

Q. Did you store the information in the Gold source copies?

A. No, I did not.

Q. Why not?

A. That wasn't my job, and I don't believe I had access to that folder.

Q. Generally speaking, who had access to the DevLAN network?

A. Users in EDG.

Q. As of 2015 and 2016, approximately how many people had DevLAN access?

A. Probably around a hundred, give or take. It was almost exclusively AED, so the -- most of the -- all of the developers and then a few other individuals.

Q. How did users access DevLAN?

A. So, when you -- when you join the group, you would check in with ISB. ISB would create a user name and password for you, in Active Directory, and those credentials, which were unique to you, were leverage to access those resources on DevLAN.

Q. Did individual users have their own DevLAN computers?

A. Yes, they did.

Q. Where were those computers located?

A. Typically, at the desk that they worked at on a daily basis.

Q. Were those desks within the vaults you described earlier?

A. Yes.

MR. LAROCHE: Ms. Hurst, can you zoom out on 1251, please.

Q. Are the DevLAN users reflected on this diagram?

A. Yes.

Q. Where are they?

A. Right over here.

Q. Is that the bottom left corner of 1251?

A. Yes. Sorry.

Q. How were users' accesses controlled?

A. The main way was through Active Directory permissions. Again, you would be given an Active Directory username and password, and your account would be assigned to different Active Directory groups.

Q. You've said Active Directory a few times. What is Active

Directory?

A. Active Directory is a Microsoft product. Its job is user authentication and permissions.

Q. Once a user had a DevLAN account, how would they log in to DevLAN?

A. So, Typically, it would be with your Active Directory credentials.

MR. LAROCHE: Ms. Hurst, you can pull down exhibit 1251. Thanks.

Q. Were there DevLAN computers in any other CIA facilities?

A. Yes, there were.

Q. Were those facilities located overseas in foreign countries?

A. Yes, they were.

Q. How many overseas CIA facilities had access to DevLAN?

A. Two.

Q. I'm going to refer to them as Foreign Office East and Foreign Office West. OK?

A. OK.

Q. How were the computers in those offices connected to the DevLAN network?

A. They were routed over an agency network to access -- access the portions of DevLAN, and while routed over the agency portion of the network, we used what was referred to as end-to-end encryption so that any traffic over the portion of the network that we didn't control nobody else would be able to access.

Q. What do you mean by agency network?

A. So, EDG is a very small portion of the agency. We owned and maintained DevLAN, which was our network. The agency has other portion -- or other networks for other purposes that are run by, you know, somewhere -- other people in the agency.

Q. Is that the internet?

A. No, it's not.

Q. I think you also said end-to-end encryption. Is that right?

A. Yes, I did.

Q. What is that?

A. End-to-end encryption is an industry term for when you -- when you are departing your one end point, so leaving your segment of a local area network, and traveling to another end point, every -- all of the communication in between those two points is fully encrypted.

Q. Are you familiar with the term "network connectivity"?

A. Yes, I am.

Q. What does that term mean?

A. Network connectivity is the status of a machine's access to network resources.

Q. What was the network connectivity like between the DevLAN network in the CCI office and the DevLAN network located in

Foreign Office East and Foreign Office West?

A. The network connectivity within CCI's office was extremely good. It was a very fast network.

Our connection to the field sites was extremely slow and caused a lot of problems for our developers overseas.

Q. What do you mean by extremely slow?

A. The transferring of files that were not necessarily that large in size sometimes could take longer than a day, and that -- that caused issues because the -- our foreign offices had to shut everything down at the end of the day and store it. So if your transfer didn't complete in time, you had to start it the next day and try again.

Q. And how big a transfer would take about a day for the foreign office?

A. I don't remember the specifics. I remember working with Frank, where Frank was trying to transfer a file that was only a few megabytes in size and it taking hours.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1026. If we could go to the first email on this chain. Please just zoom in on the to-from line.

Q. I'm showing you another email. Do you see it on the screen there, Mr. Weber?

A. Yes, I do.

Q. Who sent this email?

A. I did.

Q. Who did you send it to?

A. Patrick.

Q. When did you send it?

A. This would have been January 27, 2016, 9:07 p.m.

Q. And the subject is Bitbucket. What is Bitbucket?

A. Bitbucket was an Atlassian product. We've been referring to it as Stash up at this point. Atlassian changed its name.

MR. LAROCHE: Ms. Hurst, can you just zoom in on the text and the classification of this email.

Q. Did you classify this email?

A. Yes, I did.

Q. What did you classify it as?

A. Unclassified.

Q. Why?

A. So, the contents of this email, where I'm talking about a blog post that Atlassian put on the internet, there's nothing damaging in this email.

MR. LAROCHE: Ms. Hurst, can you zoom out and then go to the next email in the chain, the response. Just go up one more slide. I think at the bottom of this slide, if you can zoom in on the "from."

Q. Did Patrick respond to you?

A. Yes, he did.

Q. And is this the response here?

A. Yes, it is.

Q. And when did he send the response?

A. January 28 at 4:57 a.m.

Q. Who did he send that to?

A. Myself and Josh Schulte.

MR. LAROCHE: We can zoom out. Go to the next page and zoom in, at the top, including the classification. Sorry. Just zoom out again, Ms. Hurst. I'm sorry. Just from the top down through the classification. Thank you.

Q. And at the top here, is this additional people that Patrick copied? Is that right?

A. Yes, it is.

Q. One of them is Frank. I think you referred to a Frank earlier?

A. Yes, I did.

Q. Is it the same Frank?

A. Yes, it is.

Q. Who is Frank?

A. Frank was a developer in OSB that I worked closely with. He eventually was selected for an overseas position.

Q. Did the classification level on the response by Patrick change?

A. Yes, it did.

Q. How did it change?

A. It was up to secret.

Q. Is it possible to reclassify emails when you respond to them?

A. Yes, it is.

Q. In what circumstances would that happen?

A. So, the scenario that you would up the classification of an email is when your response contained classification -- or classified information that was higher than the original sending of that email.

Q. And this has a cross-through through the classification, is that right?

A. Yes, it does.

Q. When you received this email communication, did it have that cross-through?

A. No, it did not.

MR. LAROCHE: Ms. Hurst, can you zoom out, please, and zoom in on the paragraph starting "additionally."

Q. Just read the first sentence, please, Mr. Weber.

A. "Additionally, could also get them to do some maintenance on the DevLAN field connectivity."

Q. Do you understand what he's referring to there?

A. Yes.

Q. What was he referring to?

A. This -- there was both the speed of the connection as well as they were not able to access all of the resources on DevLAN that they were supposed to be able to access.

Q. Where was Patrick working at the time he sent this email?

A. He was in Foreign Office West.

MR. LAROCHE: Ms. Hurst, we can pull that email down.

Q. Now, you talked a little bit before about administrators of the DevLAN network, is that correct?

A. That's correct.

Q. And you were also a user of that network?

A. That's correct.

Q. Generally speaking, what's the difference between a user and an administrator?

A. The administrators provide access to the services. The users are the ones that leverage the services for day-to-day activities.

Q. Generally, do administrators have broader access to the system?

A. Yes, they do.

Q. In what way?

A. They -- being administrators is a privileged position. You have the keys to the kingdom for the services that you control. You're able to modify who has access to what. You're able to turn the service on, turn it off, all sorts of things like that.

Q. Were there different types of DevLAN administrators?

A. Yes, there were.

Q. What were some of those types?

A. The DevLAN administrators kind of fell into three categories. There were your true DevLAN administrators, who were in ISB. Their job was specifically focused on the administration of DevLAN, most specifically, Active Directory and the network connectivity.

There were the Atlassian administrators, who were focused solely on the Atlassian set of products. And then you would have administrators for some of the software development resources.

Q. What do you mean by that, that last piece?

A. So, a specific example was the OSB ESXi server was meant to be a tool by developers for developers for development activities, so there were some people that could maintain the ESXi server.

Q. Let's start with the first group you mentioned, I think, network-wide administrators, correct?

A. Yes.

Q. Who were the network-wide administrators as of 2015?

A. ISB.

MR. LAROCHE: Ms. Hurst, could you please publish to the parties, the Court and the witness Government Exhibit 90.

Q. Do you recognize this?

A. Yes, I do.

Q. What is this?

A. This is another portion of the org structure of EDG.

Q. Does this fairly and accurately represent that portion of the org structure of EDG?

A. Yes, it does.

MR. LAROCHE: Your Honor, we'd offer Government Exhibit 90 in evidence.

MS. SHROFF: No objection, your Honor.

THE COURT: 90 is in evidence.

MR. LAROCHE: Thank you.

(Government Exhibit 90 received in evidence)

MR. LAROCHE: Please publish that to the jury, Ms. Hurst.

Q. You've mentioned ISB a few times. Where was ISB within the organizational structure of the group?

A. They were within SED.

Q. What was their role?

A. Their role was system administration.

Q. Did they have any development role?

A. No, they did not.

MR. LAROCHE: OK. We can pull that down, please.

Q. I think the second group of administrators you identified on DevLAN were those who were in charge of the Atlassian services. Is that correct?

A. That's correct.

Q. Was ISB in charge of the Atlassian services in 2015?

A. No, they weren't.

Q. Who were in charge of the Atlassian services as administrators in 2015?

A. Originally, I believe it was Patrick. I think in early 2015 he had still an administrative role. Eventually that transitioned to me, and I very quickly brought Josh on as an administrator.

Q. As an administrator of the Atlassian services, what types of things could you do?

A. The -- our roles and responsibilities were to keep the service up and running, to ensure the backups of the service, to provide user access to different portions of it, upgrade the system, things like that.

Q. Now, you also said, I think, the third group was certain hardware that there were administrators of. Is that correct?

A. Yes.

Q. And the example you gave was the ESXi server, is that correct?

A. That is correct.

MR. LAROCHE: Ms. Hurst, can you please publish again Government Exhibit 1290 and then just zoom in on ESXi server on the top left.

Q. As of 2015 who were the administrators of the ESXi server?

A. I believe it was myself and Josh, for sure. I think Frank was also an administrator, and Matt was also an administrator.

Q. And were all the individuals you just mentioned working within OSB?

A. That is correct.

Q. As an ESXi administrator, what types of things could you do?

A. As an ESXi administrator, your job was to be able to create new virtual machines, power them on, power them off, back them up, revert them to snapshots, things like that.

Q. You used the term "snapshot"?

A. That's correct.

Q. What does snapshot mean?

A. Snapshot is a term used with virtual machines. It is creating -- creating a backup for the running state of a machine at a given time. It's -- it's a tool that you can use to back up your data.

Q. Did you ever crate snapshots of virtual machines?

A. Yes, I did.

Q. Why?

A. The most traditional-use scenario was if we were going to upgrade the machine, you would create a backup right before upgrading. That way, if there was a problem during the upgrade, you could just revert to the snapshot and it was as if it never happened.

Q. You also used the term "revert"?

A. Yes.

Q. What does that mean?

A. Revert is a term for saying discarding the current machine's running state and returning it to a snapshot.

Q. In 2015, did ISB have a role as the ESXi server administrator or Atlassian administrator?

A. I'm sorry. What was the date again?

Q. As of 2015.

A. As of 2015, they were not -- ISB was not the administrator of the ESXi server.

Q. And what about the Atlassian services?

A. No, they were not.

Q. Why were they not acting in that administrative role?

A. ISB did not have the capacity. They didn't have enough people to handle all of their responsibilities. Nor did they have somebody that was qualified to handle the Atlassian services.

Q. Let's talk for a moment about how you would log in as administrator to the system.

A. OK.

Q. I first want to focus on the Atlassian-level administrator.

A. OK.

Q. How would you log in as an Atlassian-level administrator?

A. When you were interacting with the Atlassian service, that was typically through the Atlassian -- like the web pages that Atlassian presented, so you would navigate to confluence.devlan.net, and you would be presented with a log-in screen. You would give your Active Directory username and credential to gain access to the system, and then if you were going to do administrative activities, you would click on a portion of the web page and get prompted for a username and password again to validate that you were still the same individual.

Q. Are you familiar with the term "SSH keys"?

A. Yes.

Q. What are those?

A. SSH keys are -- it is an alternative means of authentication beyond a username and password that is more secure.

Q. Why is it more secure?

A. So, most humans have a password that is going to be, you know, between six and 12 characters, most likely. It's not -- it's not something that has that much random information in it.

An SSH key usually is around 4,096 bytes, so the amount of random information in that key allowed for a much more secure authentication.

Q. Were SSH keys used to log in as an Atlassian-level administrator?

A. Through the website, no. But to access the servers that they were running on, yes.

Q. And would that give you a different type of access?

A. Yes, it would.

Q. In what way?

A. So, the -- having access to the computer would allow us to start and stop the Atlassian service. It would allow us to upgrade it as well as access the file system, things like the backups, stuff like that.

Q. And I know you said access to the server. Is that right?

A. Yes.

Q. In this context, are you referring to a virtual server?

A. I'm -- both, depending on the product. For Confluence and Bamboo, I'd be referring to a virtual server. For Stash and Jira, I'd be referring to a physical machine.

Q. Let's just talk about that for a moment. Looking at this diagram, Confluence and Bamboo are running on virtual machines, is that correct?

A. That's correct.

Q. Is that the same thing as a virtual server?

A. Yes.

Q. Why is that?

A. "Virtual server" is not an official term, so a server is just a very powerful machine that has a specific purpose in life.

Q. So you talked about logging in through the web with a username and password as administrators, is that right?

A. Yes.

Q. And you talked about logging in to the virtual server using SSH keys?

A. Yes.

Q. Now, there's also on this page an ESXi server, is that correct?

A. That is correct.

Q. Were those different administrative privileges?

A. Yes, they were.

Q. How would you log in as an ESXi administrator?

A. There were multiple ways. The typical way was using a product called vCenter or vSphere to log in via what was effectively a web interface.

Q. How would you log in that way?

A. You would use your Active Directory credentials there as well.

Q. And was there a specific route or administrative password used to log in?

A. There was a backup route password that could be used.

Q. Was there another way to log into the server as an administrator?

A. You could SSH into the server as well as physically access the server as well; plug a keyboard into it and type a username and password.

MR. LAROCHE: Ms. Hurst, could you please --

THE COURT: Mr. Laroche, would this be a convenient time to take our morning break?

MR. LAROCHE: Yes, your Honor.

THE COURT: We'll take a 15-minute break.

(Jury not present)

THE COURT: See you in 15 minutes.

(Recess)

THE COURT: Please be seated.

(Jury present)

THE COURT: Please be seated.

Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

Q. Mr. Weber, we were talking before the break about logging in as an administrator?

A. Yes.

Q. And one of the things we were talking about was logging in to the OSB ESXi server.

A. Yes.

Q. I think you referred at one point to the word "credentials"?

A. That's correct.

Q. What were you referring to there?

A. The credentials would be a username-and-password combination. Typically, I'm referring to Active Directory credentials.

Q. Just focusing on that server for a moment, the OSB ESXi server --

A. Yes.

Q. -- how would you log in as administrator to that server?

A. Logging in to the OSB ESXi server, you would typically go through vSphere to log in and do most of the administrative functions, and you would log in using your Active Directory credentials.

Q. You said vSphere?

A. Yes.

Q. What's vSphere?

A. It was -- it's a portion -- it's a product within the ESXi tool suite that was meant to interface with an ESXi server.

Q. You also said earlier that you could log in using SSH keys, is that correct?

A. That's correct.

Q. How would you do that?

A. You would use a -- any service that ran SSH, either a Linux machine, or Windows had a tool like PuTTy installed on it, you would leverage that to create an SSH access.

Q. What's PuTTY?

A. PuTTY's just a tool on windows that does communication like SSH.

Q. And if you logged in using the SSH keys to the server, is that different than logging in using the password?

A. It's -- the SSH key was set up for root, so you would be logging in as the root user versus your admin credentials.

Q. What is the root user?

A. The root user, in this situation, "root" was kind of Linux term for the administrative account on the machine, like the default administrator account.

Q. You also mentioned there was a password for the ESXi server?

A. That's correct.

Q. Was that password stored anywhere?

A. Yes, it was.

Q. Where?

A. It was stored on OSB's passwords page for some of our services.

Q. What do you mean by OSB's passwords page?

A. OSB had a lot of virtual machines outside of the Atlassian products that had passwords on them solely because the technology required to have a password and not for security practices, so that -- these were often like test machines, and these passwords we kept on a page so that if somebody was leveraging that VM they would have the credentials they needed to log in to it.

Q. Where was that passwords page located?

A. Confluence.

Q. Was it restricted in any way?

A. It was.

Q. How?

A. It was to OSB.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1003, and please just zoom in on the top of the email, the to-from.

Q. Is this another email from the CIA, Mr. Weber?

A. Yes, it is.

Q. When was this email sent?

A. It was sent on March 31, 2015, at 8:20 p.m.

Q. Who sent it?

A. It was sent by Josh Schulte.

Q. Who was it sent to?

A. It was sent to the OSB email group.

Q. How do you know that?

A. The string NCS-IOC-EDG-AED-OSB is a user group and it's explicit in its naming. NCS was in the org chart above IOC, the rest of those are the groups that we have previously talked about.

Q. It's a lot of acronyms.

A. It is.

Q. Below that, what's the subject line?

A. OSB.DevLAN.net VM credentials.

Q. What's OSB.DevLAN.net?

A. That was the OSB ESXi server.

MR. LAROCHE: Ms. Hurst, if you could please zoom out and then on to the text of the email.

Q. Can you read the first sentence, please?

A. "I've modified the OSB's ESXi server page to contain the passwords and other information directly instead of through the OSB's passwords page; also updated the permissions to be restricted to everyone outside of OSB."

Q. Do you understand what he's referring to by OSB's ESXi server page?

A. Yes.

Q. What's he referring to?

A. It was a second page created later to contain information specifically to the ESXi server and the administration of that.

Q. And do you understand what he means by updated the permissions to be restricted to everyone outside of OSB?

A. This was him saying that only people within the OSB -- within OSB would have access to read this page.

Q. Now, is this the same ESXi server that as of 2015 was running Confluence and Bamboo?

A. Yes, it was.

MR. LAROCHE: We can take that down. Thank you, Ms. Hurst.

Q. Now, you've been testifying for quite a while now about DevLAN, is that correct?

A. Yes.

Q. About its infrastructure and hardware and accesses, is that right?

A. Yes.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1251.

Q. Other than testifying today, have you ever spoken publicly about DevLAN?

A. No, I have not.

Q. Why not?

A. The DevLAN -- the setup of DevLAN was classified, and testimony about it or any discussion about it would give an adversary, if they overheard that discussion, an adversary insight into how the network was set up, what type of technology it was running, things like that. This would create a risk for the system because that's the first information you need to effectively attack a target system.

Q. One of the parts of DevLAN you talked about was Hickok. Do you recall that?

A. Yes.

Q. Other than testifying today, have you ever spoken publicly about Hickok?

A. No.

Q. Why not?

A. The same reason.

Q. Is the DevLAN network still being used today?

A. No, it is not.

Q. When did DevLAN stop being used?

A. March 7.

Q. Of what year?

A. 2017.

Q. Why did it stop being used?

A. The disclosure of the WikiLeaks led to DevLAN essentially being seen as a crime scene. We all stopped touching our computers. The FBI came in and began confiscating all of the equipment, and DevLAN ceased to exist.

Q. After the CIA stopped using the DevLAN network, did you talk about it publicly?

A. No, I did not.

Q. Why not?

A. The -- even though DevLAN was eventually replaced by another network, talking about DevLAN would still give an adversary insight into the capabilities that the system administration team had, and assuming you had the same system admin team in place, an adversary would have the knowledge that they would use the same technologies that they've used in the past, because that's what they know.

Q. You've used the word "adversary" several times?

A. Yes.

Q. Who are you referring to?

A. I would most likely be referring to foreign entities that are similar to CCI who are targeting the U.S. government.

MR. LAROCHE: You can take that down, please. Thank you, Ms. Hurst.

Q. You testified earlier that the defendant became an administrator Atlassian server, is that right?

A. Yes.

Q. When did that happen?

A. I believe it was summer of 2015.

Q. And you talked earlier about the various types of DevLAN administrators?

A. Yes.

Q. What type of administrator did he become?

A. An Atlassian administrator.

Q. Did he also have a role with the ESXi server?

A. He did.

Q. What was that role?

A. He was an administrator of that. That would have been before the summer of 2015, though.

Q. I want to focus you on the Atlassian administrative privileges that he had.

A. Yes.

Q. How did it come about that he became an administrator?

A. Andrew -- I'm sorry. Patrick asked me to become an administrator of the Atlassian products, and I -- I knew a portion of what was needed for that. However, I was not a Linux administrator by background, so I asked Josh to assist me with this.

Q. What's Linux?

A. Linux is an operating system. Specifically, it was the operating system that was running the Atlassian services.

Q. What's an operating system?

A. An operating system is -- that is the software that is used for most of your operations. So, most people would recognize windows. Windows is an operating system. Linux is another -- a competitor.

Q. Did the defendant have familiarity with that operating system, Linux?

A. Yes, he did.

Q. At the point you asked him to help you with the administration of the Atlassian services, approximately how long had you worked with him?

A. That would have been about four, four or five years at that point.

Q. At that point what was your relationship like?

A. I was close to him. I considered him a friend. We worked closely on numerous products -- projects together. I trusted him. I specifically reached out to him for this.

Q. What was the defendant's role as an Atlassian administrator?

A. So, his main focus was on the Linux pieces of it, which typically meant keeping the system up to date, start -- like updating the Atlassian products. He set up the backups for us, things like that. But generally, he -- he covered everything when there was a time or a need.

Q. Who defined his role as an administrator?

A. I did.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1251 again.

Q. At the time the defendant became an Atlassian administrator, were the Atlassian services being backed up to the Altabackups?

A. No, they were not.

Q. Where were they being backed up at that point?

A. They were being backed up locally.

MR. LAROCHE: If we could just zoom in again on the ESXi server.

Q. Just to focus on Confluence, what do you mean that the backups were being backed up locally at that point?

A. Confluence had a hard drive assigned to it, and the same -- the same location. Different file path, but essentially the same location the original data was being written to the backup data was being written to.

MR. LAROCHE: Ms. Hurst, if we could zoom out again. Thank you.

Q. Did the defendant have a role in changing where the backups were stored?

A. Yes.

Q. What was his role?

A. After the Altabackup folder was created, Josh was the one that modified the Linux machines to be able to access that folder and modified the Atlassian scripts that executed the backup to write to the new location.

Q. Let's start with the scripts.

A. OK.

Q. What is a script?

A. It's a series of commands that a computer would execute.

Q. Why did he need to modify the script?

A. The scripts were set up to write in one location, the local location. It needed to be changed to the remote location.

Q. The other thing you said he did was modify the machines, is that right?

A. That is correct.

Q. How did he modify the Linux machines?

A. The Linux machines needed to have access to the remote storage location, so he ran a command called mount that would allow, allow that network location to be accessed like any other folder on the system.

Q. Are you familiar with the term "mount point"?

A. That's correct -- yes, I am.

Q. What's a mount point?

A. A mount point is essentially the -- like the information needed to say, you know, this either hard drive, remote location, whatever, is connected to this computer and this is how you access it.

Q. Did the defendant help create mount points for the Altabackups?

A. Yes.

Q. What did he do?

A. He ran the mount command, which is what's used to create a mount point.

Q. What was the purpose of those mount points?

A. To ensure that the VMs had access to the NetApp location.

Q. You said VMs. What do you mean by that?

A. The Confluence VM, Bamboo VM or the Stash server or the Jira server.

Q. Where were those mount points located?

A. The mount points were located within the operating system on its file system.

Q. Did each Atlassian service have its own mount point?

A. Yes, that's correct.

Q. Why would they each need their own mount point?

A. They were each running on their own operating system.

Q. Could regular DevLAN users access those mount points?

A. No.

Q. Why not?

A. They didn't have access to them, and they didn't -- we didn't publish the location of them.

Q. Could regular DevLAN users access the backups in any other way?

A. No, I don't believe so.

Q. Could an Atlassian administrator access the Altabackups using those mount points?

A. That is correct.

Q. How?

A. You -- if you log in to the virtual machine itself or the physical machine and -- you'd be able to navigate to the mount point just like you would navigate to any other folder on the system.

Q. And once you went to the mount point, where would that take you?

A. The NetApp storage location.

Q. For the Altabackups?

A. Correct.

Q. After the defendant helped set up the mount points for the Altabackups, did you tell the other developers about the Altabackups?

A. No, I did not.

Q. Why not?

A. There was no reason to publish that information. The other developers wouldn't care.

MR. LAROCHE: Ms. Hurst, we can put pull that down. Thank you.

Q. Now, you said in 2015 the infrastructure support, ISB was not acting as the administrator of the Atlassian services, is that right?

A. Yes, that is correct.

Q. Did you have discussions with the defendant about that?

A. Yes.

Q. When, approximately, did those discussions occur?

A. I would -- it's safe to say that it was pretty much the extent, every single day that we were doing administrative activities via Atlassian.

Q. Could you describe those discussions?

A. The Atlassian administration duties were an additional duty as assigned. It was not our day-to-day job, and it distracted us from our day-to-day job, so it was, you know, not something that we looked forward to doing and did not want to be doing it.

Q. Did the defendant complain about the fact that ISB was not acting as the Atlassian administrator?

A. Yes.

Q. What types of things would he say?

A. It would be along the lines of, you know, we would be complaining about the fact that we would have deadlines on other projects but we're focused on fixing something in the Atlassian product or doing something. It was an significant amount of additional work, so the complaints were along those lines.

Q. Other than the defendant's complaints about ISB's roles, did the defendant make any other complaints about the Atlassian services on DevLAN?

A. No.

Q. Did the defendant ever complain that the Atlassian services were vulnerable to theft?

A. No.

Q. Are you sure about that?

MS. SHROFF: Objection, your Honor.

THE COURT: Overruled.

MS. SHROFF: It's hearsay.

THE COURT: Overruled.

BY MR. LAROCHE:

Q. Are you sure that the defendant never made any complaints that DevLAN was vulnerable to theft?

A. Yes.

Q. Why?

MS. SHROFF: Objection.

THE COURT: Overruled.

A. If he had complained to me about the Atlassian products being vulnerable to theft, I would have told him to fix it. The Atlassian products were our responsibility, and if he had highlighted an issue with that, I would have made it our primary focus to fix that.

MR. LAROCHE: Ms. Hurst, can we please publish

Government Exhibit 1012, please. If we could just focus on the bottom to-from line.

Q. Is this another email sent from the CIA, Mr. Weber?

A. Yes, it is.

Q. Who sent this email?

A. Josh.

Q. And when did he send it?

A. This would have been August 11, 2015, at 7:37 p.m.

Q. Who did he send it to?

A. This would have been sent to the email group for AED, and he also copied the email group for ISB.

Q. What's the subject line?

A. Complete Atlassian server outage.

Q. This was 2015, is that correct?

A. Yes.

Q. Was he acting as the Atlassian administrator at this time?

A. Yes, he was.

MR. LAROCHE: Could you zoom out to the text of the email, please.

Q. Could you summarize what he's saying in this email?

A. Yes. So, at this time if a user tried to log in to any of the Atlassian products, they would not have been able to, so essentially the Atlassian products were down for use. This was due to an issue connecting to the Active Directory server that Crowd needed to be able to provide access to the products.

Q. Why did you need ISB's help to resolve this issue?

A. ISB was the ones who ran the Atlassian products -- sorry, Active Directory. And this was an issue querying the Active Directory platform.

MR. LAROCHE: Could we zoom out for a second, Ms. Hurst.

Q. Was this problem resolved?

A. Yes, it was.

Q. How do you know that?

A. The next email, which I sent, says the log-in issue has been resolved.

MR. LAROCHE: We can pull that down. Thank you.

Q. Were there discussions about transitioning Atlassian administration to ISB?

A. From the day we brought it into -- into EDG.

Q. How often did you have those discussions?

A. Numerous. I would say monthly, most likely.

Q. Did that transition happen quickly?

A. No, it did not.

MR. LAROCHE: Let's look at Government Exhibit 1017. Could we just focus on the top, to-from line.

Q. Is this another email from the CIA?

A. Yes.

Q. Who sent it?

A. I did.

Q. When did you send it?

A. This would have been October 2015, October 6, 2015.

Q. Who did you send it to?

A. José.

Q. Where did José work at the time?

A. He was in ISB.

Q. Did you copy anyone on this email?

A. Yes, I did.

Q. Who did you copy?

A. Robert, Sean and Josh.

Q. Who's Sean?

A. Sean was my branch chief.

Q. Which branch?

A. He was chief of OSB.

Q. And the subject is infrastructure running on OSB's server, is that right?

A. Yes.

Q. Is this the ESXi server you referred to earlier?

A. Yes, it is.

MR. LAROCHE: If we could just zoom out for a second and then zoom in on the first paragraph.

Q. Read the first sentence, please.

A. "Below is a list of what we have running on our server, all of which we are looking to migrate to you guys when you have the horsepower."

Q. What did you mean by that?

A. If I recall correctly, ISB was standing up some new ESXi server infrastructure. Once they had that server infrastructure in place, that's what I mean in terms of horsepower.

Q. And can you read the second sentence, please?

A. "The list is in priority order, but the three in red should be considered high priority since they contain data needed for day-to-day operations (*i.e.*, the pitchforks come out when they go down)."

MR. LAROCHE: Could we zoom out, Ms. Hurst, and could we zoom in on the three in red. Thank you.

Q. Starting at the top, it says machine at the top left?

A. Yes.

Q. What's that referring to?

A. In this case it was the virtual machine running Confluence.

Q. And then below that there's another machine?

A. Yes.

Q. What's that?

A. Bamboo.

Q. Were these the virtual machines running on the ESXi server?

A. Yes, they were.

Q. When you talked about being an Atlassian administrator, did you have Atlassian administrative services for these virtual machines?

A. Administrative access to these machines?

Q. Yes.

A. Yes, that is correct.

MR. LAROCHE: We can zoom out.

We can pull this email down.

Q. After you sent this email, did ISB move Confluence and Bamboo to their infrastructure?

A. Not immediately. It took a significant amount of time.

MR. LAROCHE: Let's look at Government Exhibit 1024 and just zoom in on the to-from at the top.

Q. When was this email sent?

A. January 14, 2016.

Q. Who sent it?

A. Josh Schulte.

Q. And who did he send it to?

A. This was sent to the AED group as well as the ISB group.

Q. And what was the subject of this email?

A. Atlassian support transition to ISB.

MR. LAROCHE: If we can zoom out for a second and then zoom in on the text of the email.

Q. Could you read the first sentence, please?

A. "We are currently transitioning the Atlassian product support from OSB to ISB (POC Rufus)."

Q. Who is Rufus?

A. Rufus was somebody hired by ISB to specifically manage the

Atlassian products.

Q. Did that transition happen in January of 2016?

A. No, it did not.

Q. Why not?

A. Rufus departed after a couple of weeks working with EDG.

MR. LAROCHE: You can pull that down.

Q. Now, in addition to helping to design and run the Atlassian services, did the defendant also develop cyber tools?

A. Yes, that is correct.

Q. Generally speaking, what types of cyber tools did the defendant work on?

A. Josh's main focus was on tools for operations when we had physical access to a target machine.

Q. What do you mean by physical access?

A. Physical access would be when an agency officer or asset was willing to touch a machine for us, maybe type on a keyboard, maybe plug in a thumb drive into it, or walk off with the machine.

Q. Did the defendant work with other developers on some of his projects?

A. Yes.

Q. Do you know a developer named Amol?

A. Yes, I do.

Q. What branch within the group did Amol work in?

A. For the majority of his time with EDG, it was OSB.

Q. How often did you interact with Amol while he was with OSB?

A. Pretty much daily.

Q. Would you describe those interactions?

A. I would consider Amol a friend. We talked often. We -- we collaborated together. At the time Amol was hired, I had a project that a significant portion of my career had been spent on but I was transitioning off of, and I selected Amol to take over that project.

Q. Did Amol start working with the defendant on projects?

A. Yes, he did.

Q. Approximately when did he start doing that?

A. I believe it was almost immediately.

Q. Was there a specific project that he assisted the defendant with?

A. Yes.

Q. What was that project called?

A. Brutal Kangaroo and Drifting Deadlines.

Q. Did you observe the defendant and Amol interact?

A. Yes.

Q. How often, roughly?

A. I sat next to Josh and Amol, so any time I was at my desk and they were interacting, I would witness it.

Q. Could you describe those interactions.

A. They -- they ran the gamut. Sometimes they were completely professional, back and forth on how to approach a problem, but oftentimes, they were less than professional. And Josh and Amol did not get along personally.

Q. Did those interactions change over time?

A. It was a continuous downhill relationship.

Q. What do you mean by downhill relationship?

A. So, Josh and Amol rubbed each other the wrong way. That was obvious early on, and there was increasing animosity between the two of them as long as they were working together.

Q. Did you attempt to intervene between them?

A. Numerous times.

Q. How did you attempt to do that?

A. I would often talk to either Amol or Josh after a less-than-professional interaction and try and tell them to, you know, knock it off or calm down.

Q. Now, you said one of the tools that they were working on together was Drifting Deadlines, is that correct?

A. Yes.

Q. In early 2016, did an issue arise regarding Drifting Deadlines?

A. Yes.

Q. What happened?

A. Drifting Deadlines was supposed to meet a specific operational need. COG needed it as soon as possible. The tool was aptly named because it was constantly missing delivery milestones and deadlines, so COG requested that EDG create another, similar capability through an external contractor.

Q. What do you mean by that?

A. We paid a external company to create a tool for us.

Q. Did you talk to the defendant about that?

A. Yes.

Q. What did he say?

A. Josh was offended by this, for multiple reasons. One, he saw it as a, like he saw it as a lack of trust in him as a developer, that he would not be able to deliver the capability in time. But he also thought that the government was going to be defrauded because his and Frank's hard work, he thought, was going to be given to this contractor to be, in turn, sold back to the U.S. government.

Q. Was that true?

A. No, it was not.

Q. How do you know that?

A. That's not the way the contract was set up. The contractor was going to get capability that they would incorporate into their tool, but that was not going to be charged to the U.S. government. We have --

MS. SHROFF: Your Honor, we object to this testimony.

THE COURT: Overruled.

MS. SHROFF: It's not from something he personal his knowledge.

THE COURT: Don't interrupt. It's overruled.

A. We also have people in the agency whose job is to manage these interactions with contracts on a daily basis, and their job is to make sure that everything is in the best interests of the government.

Q. Did there come a time when there was a meeting about this contractor issue?

A. Yes.

Q. When, approximately?

A. It was, I believe, in April of 2016, early 2016.

Q. Who participated in that meeting?

A. The meeting was intended to be between the contractor, the -- my branch chief, Sean, Frank, as well as that government POC that I referenced earlier.

Q. Did the defendant participate in this meeting?

A. Yes, he did.

Q. Was he invited to the meeting?

A. No, he was not.

Q. How do you know he was not invited to the meeting?

A. I was -- again, I sat next to Josh. I also sat next to Frank. I was there when Sean came to get Frank to go to this meeting. Josh requested to attend. He was told not to go, and Josh said that he was going to go anyway.

Q. Did he say anything else to Sean at that time?

A. I remember it being along the lines of fuck you, I'm going anyway.

Q. After the meeting, did you speak with the defendant?

A. Yes.

Q. Did you talk about this issue again?

A. Yes.

Q. What was his demeanor like during those interactions?

A. So, I had a conversation with him, talking about how -- I was trying to get him to realize that the actions he took were a slap in the face to Frank and Sean, somebody that I respected greatly, and that he needed to trust in them, that this was doing the right thing and that, furthermore, his actions were -- you know -- he was burning bridges. He was making it hard so that people would not want to work with him in the future, things like that.

Q. Why did you say it was a slap in the face to Frank and Sean?

A. So, Frank and Sean, numerous times, explained to Josh was going on and that it was OK, and Josh was telling them that they were wrong.

Q. How did he react to your conversations with him about this?

A. Sort of a lot of similar conversations like this with Josh, he -- he would often acknowledge my viewpoint, and then we would move on.

Q. Around this time, did you also talk to the defendant about someone named Karen?

A. Yes.

Q. Who is Karen?

A. Karen was our group chief, chief of EDG.

MR. LAROCHE: If we could just publish Government Exhibit 89 again.

Q. So where did Karen fall within this organizational chart?

A. She would have been in charge of EDG.

Q. How many levels of management were between you as a developer and Karen as chief of EDG?

A. So, it would have went my branch chief, the division chief and deputy division chief and then deputy group chief and then Karen, the group chief.

Q. What types of things would the defendant say about Karen?

A. He --

MS. SHROFF: Objection as to hearsay.

THE COURT: Overruled.

A. He often was derogatory to her. He did not -- he did not agree with the direction of her leadership AND would often vocally state that.

Q. What do you mean by derogatory towards her?

A. Comments like dumb bitch would occasionally be thrown around.

Q. Did you respond to him about that?

A. Yes.

Q. What did you say?

A. I -- again, I would counsel him often on his actions. I respected Karen a great deal, and I thought she was one of the better group chiefs we had had, so I was trying to get him to understand the realities.

Q. How, if at all, did the defendant respond to that?

A. Very similar to other conversations I had with him. You know, he would acknowledge my viewpoint, not necessarily change his actions after the conversation.

MR. LAROCHE: Ms. Hurst, we can pull that exhibit down. Thank you.

Q. We just talked for a minute about an issue with Drifting Deadlines?

A. Yes.

Q. That occurred in early 2016, is that right?

A. Yes.

Q. Around the time of this issue, was the defendant still working with Amol?

A. Yes, I believe so.

Q. Did you observe any changes in their relationship?

A. It -- it was extremely strained at this point in their relationship.

Q. Did there come a time when you observed an argument between them?

A. Yes.

Q. When, approximately, did that happen?

A. I believe it was if not immediately following the meeting that we just talked about or the next day. Josh and Amol got into an argument about Josh's actions during -- during that meeting and the fact that he forced himself into that meeting, and it got heated.

Q. Did you attempt to intervene in the dispute?

A. Yes.

Q. How did you attempt to intervene?

A. I told them both to stop it. Specifically, I told Josh to be the bigger man and walk away from the argument.

Q. What, if anything, did he say in response to that?

A. Josh said, We all know who the bigger man is, in reference to Amol's weight.

Q. What did you understand the defendant to mean by that?

A. He was calling Amol fat.

Q. What, if anything, did you do in response to this interaction?

A. I had a very long discussion with Josh immediately after, trying to get him to realize that he was doing everything in his power to make sure any relationships he had within the agency were burnt, and that this was going to make it hard for people to work with him in the future and it's going to make him hard to be promoted.

Q. How did he react to that conversation?

A. Same as always, like he was still a little bit heated, he acknowledged my viewpoint, and we moved on.

Q. Did you tell anyone else about the interaction you observed between Amol and the defendant?

A. The conversation we had was not in a private location, so some people overheard it. We -- we talked about the interaction in general as well the next day.

Q. Did there come a time when you talked to Sean, the branch chief, about it?

A. Yes.

Q. When, approximately?

A. I believe it was the next day.

Q. And what happened?

A. I went into Sean's office, and I wanted to know if he wanted me to take a more active role in trying to get Amol and Josh to play well together. And at that point Sean told me that it was beyond us now.

MS. SHROFF: Objection, your Honor. Continued hearsay.

THE COURT: Overruled.

Q. After that conversation with Sean, did you learn that the defendant had made a complaint against Amol?

A. Yes.

Q. How did you learn that?

A. I don't remember how I first learned it, if it was just through talking to the other developers who had already discovered it, if I was officially told about it from management, or if I saw Josh's complaint.

(Continued on next page)

Q. Did you ever review the defendant's complaint against Amol?

A. Yes, I did.

Q. Did the defendant try to show it to you?

A. He did, yes.

Q. Did the defendant try to show it to others in the branch?

A. Yes.

Q. What, if anything, did you see in terms of how others in the branch reacted to that?

A. The other -- the other members of the branch were annoyed by the situation.

Q. Why?

A. They --

MS. SHROFF: Objection.

THE COURT: Overruled.

A. They felt like they were getting --

MS. SHROFF: Objection.

THE COURT: Overruled.

A. They felt that they were being pulled into a personal issue between Josh and Amol. Furthermore, Josh's complaint specifically --

MS. SHROFF: Objection, your Honor.

THE COURT: Overruled, Ms. Shroff.

A. Josh's complaint specifically called out some of us as being targets of Amol as well, which was false.

Q. Did there come a time when you actually saw that complaint?

A. Yes.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1038 and page four of that exhibit.

Q. Mr. Weber, do you recognize this?

A. Yes, I do.

Q. Do you recognize the handwriting?

A. Yes, I do.

Q. Whose handwriting is it?

A. Josh Schulte's.

Q. Is this the complaint you were referring to earlier?

A. Yes, it is.

Q. If we can go to the next page. Mr. Weber, have you seen this next page?

A. Yes, I have.

Q. Is this, from your view, a typed up version of the handwritten complaint?

A. Yes, it is.

Q. So let's focus on this one. It is a little easier to read.

A. Okay.

Q. If we can focus on the first paragraph, please.

A. Do you want me to read it?

MS. SHROFF: Your Honor, could the government clarify who typed this up, and when it was typed and when it was created?

THE COURT: Mr. Laroche?

MR. LAROCHE: It is attached to the e-mail that's been entered into evidence.

MS. SHROFF: That does not clarify the issue, your Honor.

THE COURT: That's the best we can do.

Q. Please read the first sentence.

A. "Dating back to August of 2015, Amol has made very derogatory and abusive comments to myself and my colleagues."

Q. You ever observe Amol make very derogatory or abusive comments to his co-workers?

A. No.

Q. Did you ever observe the defendant make derogatory or abusive comments to his co-workers?

A. Yes.

Q. Without discussing the substance of those comments, how often did he do so?

A. It was not a regular occurrence. But, Josh, Josh's poking of fun at other developers would occasionally cross a line.

Q. Please read the second sentence.

A. "These dark and disparaging comments include 'I wish you were dead,' 'I want to piss on your grave,' 'I want to dance on your grave,' 'I wish you'd die in a fiery crash and burn, oh I would be so happy.' 'I only say I wish you'd die because I really wish it were true.'"

Q. Did you ever observe Amol make these kind of comments?

A. Similar comments.

Q. Can you give some context to how these comments were made?

A. They --

MS. SHROFF: Objection.

THE COURT: Overruled.

A. It was usually after Josh had been having a long conversation with Amol about anything from the way a project could go, or things like that. It would usually be, like I said earlier, when Josh -- when Josh had set a path on something, it was hard to sway him. And the conversations could go for an extensive time, it would often exhaust you. So, Amol, after being in one of these conversations with Josh, would often, like, sigh, lean up against a wall, and just say something like this.

Q. Did the defendant ever tell you he was fearful of Amol based on those comments?

A. No, he did not.

Q. Did you ever talk to Amol about those comments?

A. No.

Q. Why not?

A. It's -- Josh never expressed a concern over it. Often Josh would actually laugh following comments like this. So, it was, just never felt a need to bring it up.

Q. If we can go to the second paragraph, please. Can you read this paragraph, please.

A. "Specifically, on Monday, February 29, 2016, during the midmorning, I walked into work to Amol berating me with comments such as 'bald asshole,' insulting my work, and stating that I will never get promoted past a 12 due to my poor work quality and work ethic. I responded stating that at least I can program. This infuriated Amol because usually people do not respond to his bullying or attempt to fight back."

Q. Did you observe this interaction?

A. No, I did not.

Q. The last sentence says "usually people do not respond to his bullying or attempt to fight back."

Did you ever observe Amol bully anyone?

A. No, I did not.

Q. If we can go to the third paragraph, please. Can you please read that.

A. "For the remainder of Monday and into Tuesday, Amol was very visibly distraught and upset. His behavior was out of the ordinary, and he was unusually quiet. On Tuesday, March 1st, 2016, during the midmorning, I noticed Amol about to leave his work station. I turned, facing away from him, and inquired about a project we were working on. The next thing I knew, Amol was directly behind me, unusually close, towering over me. I was caught offguard and afraid. He then, through gritted teeth, angrily said, 'I wish you were dead, and that's not a threat, it's a fucking promise.' I was afraid that he might stab me or assault me in some way. I was frightened and very concerned especially based on his behavior. I thought he may harm myself or others, so I contacted security at the end of the day to report these events."

Q. Did you ever see Amol do any these things?

A. No.

Q. We can pull that down.

After the defendant made these allegations against Amol, did you talk to the defendant about them?

A. No, I did not.

Q. Why not?

A. After seeing these allegations, I felt that Josh was lying, which I felt crossed a line, and I just was done with him. I didn't consider him a friend anymore. And I didn't want to deal with him or the drama around him.

Q. Why did you think he was lying?

A. I work closely with Amol. I didn't believe the comments, I had never seen an interaction like that, and the interactions that I did reference, or did see, I felt like Josh took significantly out of context to try and support his viewpoint.

Q. After the defendant made these allegations, were Amol and the defendant physically separated within the branch?

A. Yes, they were.

Q. How were they separated?

A. Amol was asked to move desks, and then shortly after, Josh was asked to change desks as well.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 111. If we can just zoom in on the lower left of the screen maybe to about the middle. It's over just a little bit to the right as well.

Q. Do you see OSB on Government Exhibit 111?

A. Yes, I do.

Q. Just remind us, before they were moved, where were you sitting in OSB?

A. Wait, I'm sorry. I believe this is the eighth floor.

MR. LAROCHE: We need the next page. Sorry.

Q. Do you see OSB on this page?

A. Yes, I do.

Q. This is the ninth floor, for orientation?

A. Yes, it is.

Q. Can you just circle where you sat in OSB as of 2015 and 2016.

And before the move happened, please circle first where Josh sat. And that's next to you; is that correct?

A. That is correct.

Q. Then where did Amol sit? Okay.

Can you now circle or just mark with an X first where Josh was moved to within branch.

And then with another X, where was Amol moved to within branch.

How did the defendant react to having to move desks?

A. He was offended.

Q. Why do you say that?

A. He stated that this was a retaliation against him, and it was unfair.

Q. Did he actually move desks?

A. No.

Q. Why do you say that?

A. He, he would move a couple personal items, and then return to his desk, to do his day-to-day work, until -- until Sean came and asked him again to move. And he would repeat the process. He never completed the move.

MR. LAROCHE: We can pull that down, please, thank you.

Q. The complaint that we just reviewed, was that an internal complaint to the CIA?

A. Yes, it was.

Q. Other than making that internal complaint to the CIA, did the defendant make any other complaints outside the CIA against Amol?

A. Yes.

Q. What did he do?

A. He filed a restraining order.

Q. When approximately did he do that?

A. I believe it was shortly after the incident.

Q. Where did he file that restraining order?

A. In Loudoun County.

Q. After the defendant filed that restraining order, did he and Amol remain in OSB?

A. No.

Q. What happened?

A. Amol was moved to MSB, and Josh was moved to RDB.

Q. What does RDB stand for?

A. Remote Development Branch.

Q. If we can pull up Government Exhibit 89. You see RDB on this organizational chart?

A. Yes, I do.

Q. Generally speaking, what type of work does RDB do?

A. RDB was focused on remote operations. These would have been scenarios where we had somebody communicating with a -- a target machine over the internet.

Q. Is moving to RDB from OSB a demotion?

A. No, it's not.

Q. Why not?

A. It's a sister branch. It's, it's a different focus for type of work, but it was -- it was not a junior branch in any way.

Q. How did the defendant react to being moved to RDB?

A. He -- I don't actually know. I wasn't interacting too much with him about -- I don't know how he reacted to going to RDB specifically.

Q. At the time, where was RDB located?

A. They were on the eighth floor.

Q. We can pull that down, please.

So other than reporting the incident to internal security and filing a protective order, did the defendant take any other action against Amol?

A. Yes.

Q. What did he do?

A. He filed an EEO complaint.

Q. What is EEO?

A. Equal employment opportunity.

Q. How did you learn that the defendant filed an EEO complaint?

A. I, I don't remember specifically how I was first told about it. But, eventually, I was asked to make an official statement regarding it.

Q. Why were you asked to make an official statement?

A. He referenced me in the EEO complaint.

Q. Were you asked to respond to any specific allegations?

A. All of the allegations.

Q. What do you remember responding to?

A. So, the specific ones that I remember responding to were, one, that Amol would often call my wife dumb, and secondly that Amol would make racist comments frequently.

Q. Were either of those things true?

A. No.

Q. You said that the defendant moved to RDB after filing the protective order; is that right?

A. Yes.

Q. When the defendant moved to a different branch, did he continue working on his old branch projects?

A. Not initially.

Q. Why not?

A. He was in a different branch now. He was supposed to focus on that branch's work.

Q. Did the defendant lose privileges on DevLAN to his old branch's projects?

A. Yes.

Q. What, if anything, was done to do that?

A. He was removed. If he was a project lead on projects, he was removed from that position. And in another situation, the OSB libraries, his ability to commit directly to the main branches was removed.

Q. When approximately were these changes made?

A. It would have been around the time that he changed branches.

Q. Who made them?

A. I did.

Q. Why did you make them?

A. Josh checked out of OSB, and I was following standard practices. He no longer needed access to OSB's projects.

Q. How did you make these changes?

A. I logged into the Atlassian system and changed them. I don't know if I used my administrative credentials for this or the fact that I was an admin for the projects themselves, because I was a lead for a significant portion of them. But most likely it was my administrative credentials.

Q. Did you tell the defendant before you changed his privileges to these projects?

A. No.

Q. Why not?

A. I felt it didn't need to be communicated. He was going to be working on new projects, I didn't think he would even access the old ones.

Q. I want to talk about one of OSB's projects in particular.

A. Okay.

Q. Are you familiar with a project called OSB libraries?

A. Yes.

Q. What is OSB libraries?

A. OSB was often tasked with projects that had a very short deadline to meet. Days, sometimes weeks. And to ensure that we were able to meet these deadlines, we wanted to have some of the basic components that we often wrote in a state that can be readily used.

Q. What does that mean?

A. So, I often like to say that EDG did eight things, we just did it a thousand different ways. So, if we needed to collect a file from a computer, we had code that would do that. And if you needed to collect a file, you could just incorporate that code. It was already tested. It was already, you know, well written.

Q. Who created OSB libraries?

A. It was a branch effort.

Q. Were there some developers in particular who were more involved?

A. Yes.

Q. Who?

A. Myself, Frank, and Josh were some of the major contributors early on. Matt as well.

Q. When the defendant was a member of OSB, what were his privileges on OSB libraries?

A. So, as one of the senior members of that project, he had the ability to merge code into the main branch. And by that I mean, anybody had the ability to contribute to the libraries. But before that code could be used by others, you would have to have it signed off by a certain number of developers, show it was well tested. Once those check boxes were hit, myself, Brett, Josh, or Matt would be able to click a button on the Atlassian web page and merge it in.

Q. Was the merging aspect of OSB libraries important to OSB libraries?

A. Yes.

Q. Why?

A. Once it was merged into the master branch, anybody in OSB would inherently trust that code.

Q. After the defendant left the branch OSB, did his privileges change to OSB libraries?

A. Yes.

Q. How did they change?

A. He was no longer granted access to merge in, into the master branch, but was allowed to contribute just the same as anybody else in the rest of the division.

Q. How could he still contribute to OSB libraries?

A. There was a process that we had officially outlined. You would create a separate branch of the code, you would make your modifications, and then you would submit it to review. Everybody followed this process, regardless of if you were in OSB or not.

Q. After the defendant left OSB and went to RDB, his new branch, did he maintain those privileges?

A. Yes, he did.

Q. Who changed the defendant's privileges to OSB libraries?

A. I did.

Q. After you changed the defendant's privileges to OSB

libraries, did he approach you about it?
A. Yes, he did.
Q. When approximately did he approach you?
A. I believe it was shortly after the change. I don't remember the date, though.
Q. What happened during that interaction?
A. He came up to me, asked what was going on. I informed him since he was no longer a member of OSB, that it had been decided that he would not have the ability to merge stuff into master. He disagreed with that. At which point I directed him to talk to Sean, my branch chief, his former branch chief.
Q. What was his demeanor like during this interaction?
A. During the first interaction, it -- it wasn't anything special. Very normal.
Q. You said you told him to talk to Sean?
A. Yes.
Q. Again, who is Sean?
A. Sean was my branch chief, chief of OSB.
Q. Why did you tell him to talk to Sean?
A. As chief of OSB, all of the projects were owned by him, and he was the one that had the say on what -- how things should be set up.
Q. Did the defendant talk to Sean?
A. Yes, he did.
Q. How do you know that?

A. I directed him to go talk to Sean. I saw him go into Sean's office. And then he came back afterwards to talk to me again.

Q. Could you hear the conversation he had with Sean?

A. No.

Q. After the defendant talked to Sean, did he come back to you?

A. Yes.

Q. Did you talk to him again?

A. Yes.

Q. What did he say?

A. He told me that Sean had said that his access should be returned, and that I should go and do it.

Q. How did you respond?

A. I told him that I would talk to Sean, because that was not my understanding of the situation.

Q. Did he respond to that?

A. Yes. He told me that I might as well go and do it, because it was going to happen one way or another.

Q. What did you understand the defendant to mean by that?

A. I took it as a threat.

Q. Why?

A. The "one way or another" seem very much like an ultimatum that he was going to do things his way, regardless of what was said.

Q. Did you talk to Sean after speaking with the defendant?

A. Yes.

Q. After speaking with Sean, did you give the defendant his administrative accesses back to OSB libraries?

A. No.

Q. Why not?

A. Sean disagreed with Josh's recollection of the conversation, and said that Josh was not supposed to have those accesses. He asked that I e-mail Josh explaining exactly how things are meant to be.

Q. After you spoke to Sean, did you e-mail the defendant?

A. Yes, I did.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1061. Then go to the first e-mail in this chain. Just go up one more page first for a second. The from line is at the bottom.

Q. Is that the e-mail you sent?

A. Yes, it is.

MR. LAROCHE: We can zoom out and go to the next page.

Q. When did you send this e-mail?

A. This would have been April 14, 2016.

Q. Was that on the same day that you had the conversation you were just discussing?

A. Yes, it was.

Q. What time did you send it?

A. 3:30 p.m.

Q. Who did you send it to?

A. I sent it to Josh.

Q. Who did you copy?

A. I copied Sean, chief of OSB, Tony, who was deputy division chief for AED, Richard, and Frank.

Q. Who is Richard?

A. I don't know who Richard is.

Q. Who is Frank?

A. Frank was one of the main developers of the libraries.

Q. What was the subject line?

A. OSB libraries.

MR. LAROCHE: If we can zoom out. And then zoom in on the text of the e-mail.

Q. If can you read the first line and the first bullet.

A. "Josh, I discussed things with Sean and this is the situation."

Q. Then just the next bullet.

A. "In the short term, the OSB libraries remain an OSB project and are under Frank Stedman and my guidance."

Q. What did you mean by under Frank Stedman and my guidance?

A. We would continue to lead the OSB libraries.

Q. Can you please read the next bullet.

A. "You are free to contribute to the libraries by creating a branch and following the pull request model that is in place."

Q. What did you mean by that?

A. This is the process that everybody followed to contribute code to the libraries.

Q. Can you please read the next bullet.

A. "We are hoping to move the libraries to Kevin's authority to make them officially an AED level resource."

Q. Who is Kevin?

A. He was the, he was the tech director for AED.

Q. What did you mean by "make them officially an AED level resource"?

A. We felt that the libraries were a very good idea and could be leveraged by other people in the division. And we wanted to see it grow.

Q. Then please read the next bullet down.

A. "When Kevin takes over, and if he desires for you to have direct authority for the two long lived branches, then we will give you commit access to master and develop."

Q. What type of access were you talking about potentially giving back?

A. This would be his ability to merge code into the master and develop branches.

Q. What did you mean by "when Kevin takes over"?

A. We wanted to, again, make this Kevin's responsibility to chart the direction of the libraries as well as maintain the authenticity of the code. And so, we wanted -- it was in the works to have him become lead of the project.

Q. Please read the last sentence of the e-mail.

A. "Until something officially changed, you must follow the pull request model and leave it to either Frank or me to complete the merge."

Q. What did you mean by "you must follow the pull request model"?

A. Again, we had a well-laid out process that anybody, including Frank and myself, would follow for contributing code to the main branches. You would write what you wanted to change, and then you would put it up for review. Once enough people reviewed it and felt it met quality thresholds, it would be merged into the main branch.

Q. Just zoom out again. This e-mail was sent at 3:30 p.m., is that correct?

A. That is correct.

MR. LAROCHE: Ms. Hurst, if you can go to the next e-mail in this chain. Just zoom in on the to from.

Q. Who sent this e-mail?

A. Josh did.

Q. When did he send it?

A. He sent it on the same date, April 14, 2016, at 3:39 p.m.

Q. Did he copy all the same people that were on other e-mail?

A. Yes, he did. I don't know if Kevin was on the first e-mail, technically.

Q. If we can go to the text of this e-mail. Read the first sentence, please.

A. "Hey guys, thanks for the e-mail. I know soon Richard will relieve Sean of his official duties."

Now I remember who Richard is.

Q. Who is Richard?

A. Richard was a senior developer in OSB. Sean was moving on, he accepted a new position, and Richard was going to take over temporarily as chief of OSB.

Q. Can you read the next sentence.

A. "I've talked with Anthony and Sean a bit about working on transitioning some of my old projects, but haven't specifically talked about the OSB libraries until now."

Q. And the next sentence, please.

A. "Since the OSB libraries were initially my idea that stemmed from Brutal Kangaroo, and I've spent a lot of time and effort managing and helping administer them, I'd like to stay on along with Frank and Jeremy as helping administering them."

Q. Were the OSB libraries the defendant's idea?

A. No.

Q. Whose idea were they?

A. It was primarily mine and Frank's.

Q. At the time he sent this e-mail, had you already had a conversation with him about OSB libraries?

A. Yes. It was the conversation we just talked about.

Q. Had he already had a conversation with Sean about OSB libraries?

A. Yes.

Q. Can you read the next sentence, please.

A. "Especially considering that the goal is to move these to AED and allow Kevin to admin them, I feel like my intimate knowledge with the libraries would be beneficial to this process."

Q. And next sentence.

A. "I believe I should still have sufficient time to help with the libraries, and it would help propagate the libraries by having people on other branches working together on them."

Q. And just skip to the last sentence that starts "so" at the bottom.

A. "So if OSB and RDB would be okay with this, I would like to continue my active role with the libraries."

Q. At the time he sent this e-mail, had you spoken to Sean about the libraries?

A. Yes.

Q. What did Sean say about his accesses to the libraries?

MS. SHROFF: Objection as to hearsay.

THE COURT: Overruled.

A. Sean was completely okay with Josh contributing to the libraries following the official process, but wanted Frank and I to be the ones that managed merging stuff into master and develop until Kevin took over and made a decision on that.

Q. Had you communicated that with the defendant?

A. Yes.

MR. LAROCHE: You can pull this e-mail down.

Q. After the defendant sent this e-mail, what, if anything, did you do with respect to OSB libraries?

A. I went back in and looked at the audit logs on the libraries.

Q. What are audit logs?

A. Audit logs can be anything that contain information. Specifically in this scenario, it was logs that said when permissions were assigned, removed, changed; things like that.

Q. What, if anything, did you see in the audit logs with respect to OSB libraries?

A. Following this e-mail, Josh changed the permissions to give him access to the master and develop branches again.

Q. How do you know it was the defendant who changed the project permissions to OSB libraries?

A. The change was done by Josh's Active Directory account, which only he would have known the user name and password to.

Q. What privileges did the defendant use to change his accesses to OSB libraries?

A. He used his administrative privileges on the Atlassian products.

Q. Were the defendant's actions consistent with CIA policy?

A. No, they were not.

MS. SHROFF: Objection.

THE COURT: Overruled.

Q. You can answer again.

A. No they were not.

Q. Was the defendant allowed to do this as an administrator of the Atlassian services?

A. No, he was not.

Q. Why not?

A. You are given a lot of ability as an administrator, but everything that we did would be at direction.

Q. Had the defendant ever done anything like this before?

A. No.

Q. Did you tell anyone about the defendant using his administrative privileges to reinstate his access to OSB libraries?

A. Yes.

Q. Who did you tell?

A. I immediately informed Sean.

Q. Why did you tell Sean?

A. He was my immediate leadership.

Q. Why did you tell him immediately?

A. Because I saw this as a breach of the security rules, and that this was an abuse of Josh's administrative privileges.

Q. Was this an urgent issue in your view?

A. Yes, it was.

Q. Why?

A. Josh showed that he was no longer somebody that could be trusted with his administrative credentials. Because he was willing to do what he wanted to, versus what he was told to do.

Q. Was that problematic for someplace like the CIA?

A. Yes.

Q. Why is that problematic in the CIA?

A. The CIA, we have access to a lot of very damaging information. And the only way we are able to work with this type of information is by being trusted to handle it appropriately.

Q. After speaking with Sean, did you talk to anyone else about this issue?

A. Yes.

Q. Who?

A. Anthony and I believe Mike.

Q. You said Anthony. What was Anthony's position?

A. Anthony was the deputy division chief, so he was Sean's immediate supervisor.

Q. Who was Mike?

A. Mike was the deputy group chief.

Q. Let's pull up Government Exhibit 89. Let's start with Mike. What was Mike's role within this organizational chart?

A. Mike was the deputy group chief for EDG. So he was Karen's second.

Q. What about Anthony?

A. Anthony was the deputy division chief for AED.

Q. Again, what about Sean, where did he sit?

A. Sean was chief of OSB.

Q. How often did you have interactions with someone at Mike's level?

A. I was more often than others -- I would not interact with him often on stuff like this. I had other positions where I would occasionally advise group level management about technical topics.

Q. On this issue in particular, can you describe your conversations with those individuals?

A. I relayed the facts of what happened. And then I was asked to leave.

Q. After that conversation occurred, were you asked to do anything in the days that followed?

A. Yes.

Q. What were you asked to do?

A. I was asked to come in with MSB -- sorry. ISB at the time. They, it had been decided that ISB would take over the administrative role of the Atlassian products, and I was there to assist them in doing that.

Q. What day of the week did you go in?

A. Saturday.

Q. Is Saturday a typical day to work within your group?

A. No, it is not.

Q. Why did you go in on a Saturday for this issue?

A. Two reasons. One, there was going to be a downtime of the Atlassian products. We did not want this downtime to interfere with the daily activities of the software development team. And two, we wanted to make sure that we could do this without Josh's interference.

Q. Why did you want to make sure you could do it without Josh's interference?

A. We didn't trust him to not interfere.

Q. Did anyone else work with you on that Saturday?

A. Yes.

Q. Who?

A. It would have been Dave and Tim.

Q. Who is Dave and Tim?

A. They were system administrators within ISB.

Q. Did you have any instructions about what you were supposed to do that day?

A. Yes.

Q. What were you supposed to do that day?

A. I was there to answer questions that ISB might have, and oversee the transfer of administrative privileges. I was explicitly told not to do any of the modifications to the Atlassian products myself. And then after ISB was finished, to check that I did not have administrative access anymore.

Q. What administrative privileges were being changed that day?

A. The access to the Atlassian products.

Q. Why were your privileges also being taken away that day?

A. Mike and Anthony wanted to make it such that ISB was the only administrators.

Q. Why?

A. They felt it was time for ISB to take it over.

MS. SHROFF: Objection as to what they felt.

THE COURT: Overruled.

A. They felt that it was time ISB took this over. It was something that we requested numerous times. And they wanted it so that only ISB would be administration to make sure that developers developed, and system administrators handled administration.

MR. LAROCHE: If we can pull that exhibit down and put up Government Exhibit 1251, please. Please zoom in on the ESXi server.

Q. At the time in 2016, an ESXi server was running Confluence and Bamboo?

A. Yes.

Q. Who did that server belong to?

A. OSB.

Q. Who was administering that server as of April 2016?

A. It would have been myself, Frank, Matt. Those individuals.

Q. Was the plan on that Saturday to give ISB control over that server?

A. No.

Q. Why not?

A. The plan was for ISB to have control over the Atlassian services. The ESXi server that we're talking about here was going to remain an OSB resource, so there was no reason for ISB to take it over.

Q. Who was going to remain as a server administrator of that server after your weekend work on a Saturday?

A. Members of OSB.

Q. What, if any, role did the defendant have at that time as a server administrator of the OSB server?

A. None.

Q. Why not?

A. He was no longer a member of OSB.

Q. Let's focus on what you did on that Saturday. Do you remember what day that was in April?

A. I believe it was April 16.

Q. So you said that part of what you were doing was making changes to the administrative services of Atlassian, correct?

A. Yes.

Q. Before making those changes, did you do anything to the system?

A. Yes.

Q. What did you do?

A. MSB or ISB created a snapshot of the VMs before making the changes.

Q. So we're looking at Government Exhibit 1251 and we're still zoomed in on the ESXi server. What do you mean by create a snapshot?

A. Any time you're going to make like a major modification to the running state of a service, taking a snapshot gives you a safety net. So, we created a backup of that state and time before we made any modifications to it.

Q. Just looking at this screen. Was a snapshot created of Confluence?

A. Yes.

Q. Was a separate snapshot created of Bamboo?

A. Yes.

Q. We can pull that down.

After the snapshots were created, how were the administrative privileges of the Atlassian services actually changed?

A. MSB followed multiple -- they changed them in multiple areas. One, the primary ways that we had access, we, Josh and I had access to the Atlassian products, was through our Active Directory credentials. That -- the group that our accounts were part of was an Atlassian user group. We were removed from that and ISB added their members to that group.

In addition to that, we followed -- essentially, a guide that said if you are resetting access to a Linux operating system, do this, this and this. It was reset the route password, change out any SSH keys. I can't remember beyond that.

Q. We talked about SSH keys earlier.

A. Yes.

Q. Was that one of the ways that you could log in as an Atlassian administrator?

A. Yes.

Q. How did you change SSH keys?

A. In this scenario, we deleted any known keys on the system, MSB generated new keys, and then added those to the system.

Q. And you said MSB. Is MSB just another name for ISB?

A. Yeah. Sorry. Around this time, they were renamed from ISB to MSB.

Q. After the passwords, new passwords were generated, were you provided access to those passwords?

A. No, I was not.

Q. Why not?

A. I was no longer an administrator of the Atlassian product, so I was not authorized to have access to it.

Q. What about the new SSH keys?

A. The same. Same thing. I didn't have access and was not allowed access.

Q. Let's focus on the OSB ESXi server for a moment.

A. Yes.

Q. Did you take any steps on April 16 to change the privileges on that server?

A. Yes.

Q. What did you do?

A. The server had a route privilege, it was a shared password. I reset that password to something else.

Q. Why did you do that?

A. In the -- I was doing my due diligence. It was in OSB's control. Josh knew the old server password, so I felt it was right to change that password.

Q. After you changed that server password, what, if anything, did you do to OSB's Confluence page?

A. I updated the Confluence page to reflect the new password.

Q. Who had access to that page?

A. Only members of OSB.

Q. Did the defendant at that time have access?

A. I don't believe so.

Q. If we can put up Government Exhibit 1251 just for a moment. I just want to talk through what the end result of April 16 was. So I just want to start with the Atlassian services.

After the changes on April 16, 2016, who had administrative control over the Atlassian services?

A. MSB, ISB.

Q. Did you have control?

A. No, I did not.

Q. After April 16, 2016, did you have any administrative role with respect to the Atlassian services?

A. No. Outside of technically there's things like project admins, but that's outside of what would be traditionally considered an administrator.

Q. What about the defendant? After April 16, 2016, did he have any administrative role over the Atlassian services?

A. No.

Q. Let's talk about the ESXi server. If we can zoom in on that on top left, please. After April 16, 2016, who had administrative control over the ESXi server?

A. It should have been members of OSB.

Q. Did the defendant have any administrative role with respect to that server?

A. I don't believe so.

Q. You stated that that server was used for things other than running Confluence and Bamboo programs; is that right?

A. That's correct.

Q. Did that include work on other OSB projects?

A. Yes.

Q. After the defendant moved to RDB, are you aware of any need for him to have access to that server for his projects?

A. No.

Q. Did his new branch, RDB, use the ESXi server for any of its projects?

A. I don't believe so. They would not have interacted with the ESXi server directly. They might access a VM or two that was on the system. But, not the ESXi server itself.

Q. We can pull that down. Thank you.

After April 16, 2016, were developers notified about the change in administrative privileges on the DevLAN network?

A. I don't know. I believe so.

MR. LAROCHE: Let's look at Government Exhibit 1064. Just zoom in on the top to from of this e-mail.

Q. When was this e-mail sent?

A. It would have been April 18, 2016.

Q. Who sent this e-mail?

A. Anthony.

Q. Who did he send it to?

A. All of AED, ISB, as well as James.

Q. And you see there is a BCC line?

A. Yes.

Q. What does BCC mean?

A. Blind carbon copy. Anybody who received this e-mail would not see that Anthony and Michael were also on this line.

Q. Is that the same Michael you referred to as the deputy chief of EDG?

A. That's correct.

Q. What was the subject of this e-mail?

A. "Update to Atlassian products admins."

MR. LAROCHE: If we can just zoom out and zoom in on the second paragraph.

Q. Can you just read the first sentence.

A. "Following updates and changes to our -- blank -- internet system, EDG has begun to take look at our other networks to get a better understanding of our policies, etc. After a brief DevLAN audit, we realized we never quite finished transitioning the Atlassian products to SED/ISB for administration updates, etc. Therefore, to ensure that everyone in EDG was not affected while this transition was being made, SED/ISB personnel transferred all system admin responsibilities across all Atlassian products to SED/ISB removing local admin rights for all local AED branch system admins this past weekend."

Q. Was this summarizing the work you did on April 16?

A. Yes.

Q. If we can zoom in on the next paragraph, please. Just read the first sentence.

A. "As a result of this change, there are now two people in SED/ISB who will maintain and update the Atlassian suite repository for EDG."

Q. Was the defendant one of those two people?

A. No, he was not.

Q. Who were?

A. It would have been Dave and Tim.

Q. Can you read the next sentence, please.

A. "This will ensure that our entire CNE library of tools, code repository, etc. is backed up regularly. Updates to the Atlassian tool suite are scheduled and maintained, and the library remains under a common source control authority in ISB."

Q. There a reference to being backed up regularly.

A. Yes.

Q. What's that a reference to?

A. This is the backups that we discussed earlier.

Q. After April 16, 2016, did the defendant have any role administering the backups?

A. No, he did not.

Q. We can pull that down. That e-mail was sent on April 18, 2016?

A. Yes.

Q. As of that date, was the ESXi server still running Confluence and Bamboo?

A. Yes, it was.

Q. Did that change?

A. Yes, it did.

MR. LAROCHE: Can we publish Government Exhibit 1067, please. Just zoom in on the to from at the top, please.

Q. What's the date of this e-mail?

A. This would be April 20, 2016.

Q. What time was this e-mail sent?

A. 12:06 p.m.

Q. Who sent it?

A. I did.

Q. Who did you send it to?

A. All of EDG, staff and contractors.

Q. Would EDG staff include the defendant?

A. Yes, it would.

Q. What's subject of this?

A. "Scheduled downtime for Bamboo and Confluence 4/25/2016."

Q. If we can just zoom in on the text of the e-mail. Just read that into the record, please.

A. "All, on Monday, April 25 at 6 a.m., ISB will be migrating the Bamboo and Confluence servers to new hardware and will need to power them down for a limited amount of time. To ensure no work is lost, please log out of Confluence and Bamboo when you depart on Friday. If this maintenance window will cause any issues for you, feel free to contact me."

Q. Can you summarize what you meant in this paragraph.

A. So, I was asking everybody to log out of the system, so that there wasn't any unsaved work before ISB powered off the machines.

Q. Why were they going to power off machines?

A. They were going to be transitioned to new hardware off of

OSB's ESXi server.

Q. So Confluence and Bamboo would no longer being running on the OSB server?

A. That's correct.

MR. LAROCHE: We can pull that e-mail down, please, and pull up Government Exhibit 1069. Then just please zoom in on top, the to from.

Q. When was this e-mail sent?

A. This would have been April 20, 2016, at 3:58 p.m.

Q. Who sent it?

A. Robert.

Q. Who did he send it to?

A. To the EDG group, as well as ISB.

Q. Would the defendant have received this e-mail?

A. Yes, he would have.

Q. What's the subject?

A. "Atlassian suite maintenance, Monday, 25 April, 0600 to 1000 hours."

Q. If we can now just zoom in on the text of the e-mail, please. Just read the first two paragraphs to start.

A. Okay. "Good afternoon. On Monday, 25 April, from 0600 to 1000 hours, the Atlassian suite, in particular, the Bamboo and Confluence servers, will be unavailable due to maintenance. SED/ISB will be transferring data to new servers/hardware to bring DevLAN Atlassian suite under SED/ISB configuration management in accordance with EDG best practices."

Q. Can you summarize what those two sentences are saying.

A. That from 6 a.m. until 10 a.m., on 25 April, the Confluence and Bamboo VMs were going to be transferred off of OSB's infrastructure on to ISB's infrastructure.

Q. Is that the same information you had communicated earlier in the day?

A. Yes, it was. I think a little bit more detailed on the times.

Q. This is on April 20, 2016?

A. Yes.

MR. LAROCHE: If we can zoom in on the date, please.

A. Yes, April 20.

MR. LAROCHE: We can pull that down.

Your Honor, with the Court's permission can I read a stipulation?

THE COURT: Yes.

MR. LAROCHE: It is hereby stipulated and agreed by and among the United States of America, by Geoffrey S. Berman, United States Attorney for the Southern District of New York, David W. Denton Jr., Sidhardha Kamaraju, and Matthew Laroche, Assistant United States Attorneys, of counsel, and Joshua Adam Schulte, the defendant, by and with the consent of his counsel Sabrina Shroff, Esq., Edward Zas, Esq., and James Branden, Esq., that:

If called as a witness, a member of the Federal Bureau of Investigation or FBI computer analysis response team, this person known as CART Member-1, with knowledge of the matter would testify that on or about March 10, 2017, CART Member-1 was present at the office building for the Central Intelligence Agency or CIA Center for Cyber Intelligence, or CCI, located in the Washington Metropolitan area, the building known as the CCI building. While CART Member-1 was present in room 9E79 of the CCI building, CART Member-1 recovered (i) a Dell Precision computer tower that was used by the defendant to access the CIA computer network called DevLAN while the defendant was employed at the CIA and that was logged into evidence as E0001_RM9E79_FM014_tower. Known as device E0001. And (ii) a Sandisk Extreme USB device that was logged into evidence as E0003_RM9E79_FM014, known as device E0003_FM014. Device E0001 contained four hard drives, Hard Drive-1 through Hard Drive-4. Government Exhibit 1201 is a compact disc containing true and accurate copies of photographs of device E0001; Government Exhibit 1202 is a compact disc containing true and accurate copies of forensic files data recovered from Hard Drive-1; Government Exhibit 1203 is a CD containing true and accurate copy of forensic files and data recovered from Hard Drive-3; government Exhibit 1203-28 is a CD containing a true and accurate copy of a log file recovered from Hard Drive-3. Government Exhibit 1204 is a compact disc containing true and accurate copies of photographs of device E0003_FM014; and Government Exhibit 1205 is a compact disc containing true and accurate copies of forensic files and data recovered from device 0003_FM014.

If called as a witness, another member of FBI CART known as CART Member-2 with knowledge of the matter would testify that on or about March 11, 2017, while CART Member-2 was present in room 9E79 of the CCI building, CART Member-2 recovered a NetApp server containing 24 hard drives that was logged into evidence as E0018_RM9E79_24HDD, known as device E0018. Government Exhibit 1206 is a compact disc containing true and accurate copies of photographs of device E0018, and Government Exhibit 1207 is a compact disc containing true and accurate copies of forensic files and data recovered from device E0018.

If called as a witness, another member of FBI CART known as CART Member-3 with knowledge of this matter would testify that on or about March 23, 2017, while CART Member-3 was present in room 9W89A of the CCI building, CART Member-3 recovered an ESXi server that was logged into evidence as E022_RM9W89A_Dell known as device E0022. Government Exhibit 1208 is a compact disc containing true and accurate copies of photographs of device E0022, and Government Exhibit 1209 is a compact disc containing true and accurate copies of forensic files and data recovered from device E0022.

If called as a witness, another member of FBI CART, Member-4, with knowledge of the matter would testify that on or about June 9, 2017, while CART Member-4 was present in room 9E78 of the CCI building, CART Member-4 recovered a Dell Precision tower 7910 containing two hard drives that was logged into evidence as E0056_RM9E78_010, also known as device E0056. Government Exhibit 1210 is a compact disc containing true and accurate copies of photographs of device E0056, and Government Exhibit 1211 is a compact disc containing true and accurate copies of forensic files data recovered from device E0056.

Finally, if called as a witness, another member of FBI CART, CART Member-5, with knowledge of the matter would testify that on or about March 12, 2017, while CART Member-5 was present at an offsite CIA facility located in the Washington Metropolitan area, CART Member-5 recovered a NetApp server that was logged into evidence as E0012_RMLE70E, also known as device E00012. Government Exhibit 1212 is a compact disc containing true and accurate copies of forensic files data recovered from device E0012.

It is further stipulated and agreed that this stipulation, as Government Exhibit 3005, Government Exhibits 1201 through 1212, and all government exhibits identified on this document may be received in evidence as government exhibits at trial. Signed by the parties.

THE COURT: They're received in evidence.

MR. LAROCHE: Thank you, your Honor.

(Government's Exhibit 3005, 1201-1212, and all exhibits contained therein received in evidence)

MR. LAROCHE: Your Honor, if the Court is close to a break, this might be a good time to stop.

THE COURT: All right. We'll take a break now and we'll resume at 1:30.

(Jury excused)

THE COURT: See you at 1:30.

(Recess)

(Continued on next page)

AFTERNOON SESSION

1:35 p.m.

THE COURT: Good afternoon. Please be seated.

(Jury present)

THE COURT: Please be seated.

Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

Ms. Hurst, can you please publish Government Exhibit 1251.

Q. Mr. Weber, before the break, we were talking about some of the privilege changes that occurred on April 16, 2016. Do you recall that?

A. Yes.

Q. I think one of the privilege changes you recalled was the Atlassian server administrators were changed after April 16, 2016, is that right?

A. That's correct.

Q. But just you and OSB remained in control of the ESXi server, is that correct?

A. That is correct.

MR. LAROCHE: Ms. Hurst, can you just zoom in on the ESXi server.

Q. After those changes were made on April 16, 2016, were Confluence and Bamboo still being run on the OSB ESXi server?

A. Yes.

Q. Were they being run as virtual machines?

A. Yes, they were.

Q. As a server administrator of the ESXi server, what types of things could you do with a virtual machine running on a server?

A. You could power the machine on, power it off. You could delete it. You could take a snapshot. You can revert to a snapshot, things like that.

Q. And the snapshot is the same thing you were talking about earlier, which is something you created on April 16, 2016, is that right?

A. That's correct.

Q. And what did you create snapshots of that day?

A. We created snapshots of Confluence and Bamboo.

Q. What were the purposes of those April 16 snapshots of Confluence and Bamboo?

A. If we messed up the changes that we were making to the system, we wanted a point in time that we could revert back to to undo those changes.

Q. And just focusing on what those snapshots would have contained, what administrative privileges would have been contained within those snapshots?

A. So, the snapshot would have had the setup as it was before we made the change. So I would have had admin access, Josh would have had admin access. And we'd revert it back to that.

Q. And you talked about earlier access to the backups, is that correct?

A. Yes.

Q. And one of the things you talked about were the mount points?

A. Correct.

Q. And the mount points the defendant set up?

A. Yes.

Q. Where would those mount points have been?

A. They would have been in each of those VMs, the Confluence VM, the Bamboo VM.

Q. What access did you need to get to those mount points?

A. You would have needed to log in to the host operating system, which would have required access to the admin account on the host operating system.

Q. And were those accesses in place for the defendant prior to the changes on April 16, 2016?

A. Yes.

MR. LAROCHE: Let's go back to Government Exhibit 1069.

Q. We talked about this email also before the break, is that correct?

A. Yes, we did.

Q. When was this email sent?

A. This email was sent on April 20, 2016, at 3:58 p.m.

Q. What changes were going to be made on April 25, 2016?

A. The machines, Confluence and Bamboo, were going to be transferred to the new infrastructure.

Q. So the virtual machines that were running on the OSB server were getting transferred to another server?

A. That is correct.

Q. I want to show you some log files that have been entered into evidence from the defendant's computer.

A. OK.

MR. LAROCHE: Please publish Government Exhibit 1202-18, a log file from the defendant's DevLAN computer.

Q. We're going to drill down on this, but do you recognize what this is?

A. Yes, I do.

Q. What is it?

A. This is a log file that would have been generated by VMware.

Q. And what is that?

A. VMware was the company that -- they owned ESXi. They did vSphere. They did vCenter. So it's any one of those products.

Q. Generally speaking, what's a log file?

A. A log file is diagnostic information, historical information. There's different types of log files.

Q. What do log files show?

A. Depending on the log file, a security log file would show when somebody accessed certain information. You might have a service log file that would aid you in diagnosing, like, something was failing. It could be any manner of information.

Q. What does a VMware log file show?

A. In this case, an action that occurred on a VM.

MR. LAROCHE: Let's zoom in to the first three lines of the highlighted text there. That's fine.

Q. Let's start on the first line. There is a "ShowWarn:M." Do you know what that means?

A. That would have been the fact that it was showing a warning, and I don't know what the colon M means.

Q. What about what's next to that?

A. That's a time stamp.

Q. What is the time stamp of this log file?

A. It's April 20, 2016, at 5:35 p.m.

Q. And then let's go to the right of the time stamp. There's a confirm and then a colon. Could you please read that?

A. "Current state of the virtual machine will be lost unless it has been saved in a snapshot. Revert to snapshot BK4-16-2016."

Q. What is this log file showing?

A. This is a warning that would have been presented saying that if the virtual machine is reverted to this snapshot, any -- any work that had been done since that time stamp -- or that date would have been lost.

Q. And then after the warning, it says revert to snapshot. Do you see that?

A. Yes.

Q. What's that mean?

A. The -- I'm sorry. Could you repeat the question?

Q. Sure. On the first line, at the end, it says revert to snapshot?

A. Yes.

Q. What does that mean?

A. That is telling the virtual machine to restore its state to the snapshot that was taken.

Q. And then after that there's BK4-16-2016?

A. Yes.

Q. Do you know what that refers to?

A. BK is just a, what was decided to just be used as the name. And the 4-16-2016 was also included in that name.

Q. Do you understand what's that referring to, though?

A. We're saying backup 4-16-2016. We're saying, just letting anybody know who looked at the snapshot that this was taken at this time.

Q. Is that a specific snapshot?

A. It is the one that we took the morning of 4/16 before going and making the changes.

Q. So while the old administrative changes were still in place?

A. That's correct.

Q. Do you know what server this is from?

A. Yes, I do.

Q. How do you know that?

A. The next line afterwards references OSB.DevLAN.net.

Q. And where is that?

A. It's on the second or third, depending on how you're counting it, line, the one that starts with "VI client soap tran:M."

Q. And at the end there's OSB.DevLAN.net?

A. That's correct.

Q. Could you just circle that, please.

What server that is?

A. That is OSB's ESXi server.

Q. What activity is this log file reflecting?

A. This is showing that the virtual machine that was sitting on OSB's ESXi server was reverted to a snapshot at the time I referenced earlier.

Q. Which virtual machine?

A. I don't know the specific virtual machine. I believe it is -- I think in this position that I see, I don't think I see anything that references the specific virtual machine. This would have been Confluence or Bamboo, though.

Q. And why do you say Confluence or Bamboo?

A. Those were the two virtual machines that we worked with on 4/16.

Q. And what time did this activity occur?

A. This occurred on April 20 at 5:35 p.m.

Q. On April 20 at 5:35 p.m., did you revert a snapshot of Confluence or Bamboo?

A. No, I did not.

Q. Is reverting a snapshot of Confluence or Bamboo an administrative activity or a user activity?

A. It's an administrative activity.

Q. What privileges would be required to do that?

A. You would need to have a specific administrative privilege to revert to, revert to snapshot.

Q. And is that server-level privileges?

A. It would have been an ESXi set of privileges, so it's for the ESXi server.

MR. LAROCHE: You can take that down.

Q. I want to show you a file that comes from the NetApp server.

MR. LAROCHE: Please publish Government Exhibit 1207-27.

Q. Do you recognize this?

A. Yes, I do.

Q. What is it?

A. This is a directory list of the Confluence directory and the Altabackup.

MR. LAROCHE: If we could just zoom in on maybe the top five or six lines, including the title of the columns.

Q. Let's just walk through the first few lines. Just starting with -- first, where are these files located?

A. They're located in Altabackup.

Q. And just starting with the first column, what's the name?

A. The name is the -- it's Confluence_db20160201-0625.

Q. What TYPE of file is that?

A. It's a SQL file.

Q. What is that?

A. This -- SQL is a technology Confluence -- all of the data that Confluence stored was in a SQL directory.

Q. Do you see the next column that says date modified?

A. Yes.

Q. What does that reflect?

A. Date modified is any time a file-write activity occurred, so either the creation of this file the first time or a modification to the file itself.

Q. So just looking at these two files, when were they created?

A. They were created on the 1st and the 2nd around 6:30 in the morning.

Q. And then the next column says type. What is that?

A. Type is just a friendly explanation of the extension.

Q. And then the next column has size. What's that?

A. That is the size of the file on disk.

Q. The next column has date accessed. What does that reflect?

A. So, date accessed is anytime there was a read operation. This would be opening the file to view it or copying the file.

Q. And the next column has date created. What's that?

A. So, date created is the date -- the first date that that file was created on disk.

MR. LAROCHE: Can we zoom out again, please.

Ms. Hurst, if you can, please zoom in on the rows that encompass government exhibit and also keep the top rows, if we can. OK.

Q. Just focusing on the bottom for a moment, what is the bottom showing?

A. Additional files in the directory, same information that we just went over.

Q. Then there's a date modified that seems to be daily making new backups, is that right?

A. Yes.

Q. I want you to focus on the backup that was modified on March 3, 2016. Do you see that?

A. Yes, I do.

Q. Could you just circle that.

When was the backup that was created on March 3, 2016, modified?

A. It was modified at 6:29 a.m. on March 3, 2016.

Q. Let's go to the date accessed. When was the backup created on March 3, 2016, last accessed?

A. It would have been April 20, 2016, at 5:42 p.m.

Q. What types of actions would change the date accessed?

A. Opening the file to read it or copying the file.

Q. On this page, do you see any other backups that have a different date accessed than date modified?

A. No, I do not.

Q. Mr. Weber, did you access the March 3, 2016, backup on April 20, 2016, at 5:43 p.m.?

A. No, I did not.

Q. Did you copy the March 3, 2016, backup on April 20, 2016, at 5:43 p.m.?

A. No, I did not.

Q. Have you ever accessed any backup in the Altabackups?

A. The most I would have accessed the files in the Altabackup share would be to navigate to a folder like this, see that the files are getting created and using that as "backup's good" and then moving on.

Q. Have you ever copied any of those files in the Altabackups?

A. No, I have not.

MR. LAROCHE: Could we go to Government Exhibit 1207-28, please.

I'm sorry. 1207-30.

Q. Do you recognize what's on this screen?

A. This also looks like a, the backup folder, the Confluence directory.

Q. And what types of files are on this screen?

A. So, TGZ is a term for compressed, a compressed file a lot -- most people recognize -- a dot-zip file is very similar to what you see here.

Q. And what are the purposes of these TGZ folders in the backups?

A. So, these TGZ files would be the compressed contents, so everything that we just saw in the SQL stuff, or similar data, would be compressed to save file space.

MR. LAROCHE: Let's zoom in on maybe the first five or six rows, please.

Q. And again, can you circle the TGZ file that was modified on March 3, 2016.

What was the date accessed of that file?

A. The date accessed was April 20, 2016, at 5:43 p.m.

Q. Did you access this file at that time?

A. No, I did not.

MR. LAROCHE: We can pull that down.

Ms. Hurst, can you please publish Government Exhibit 1203-29, another log file from the defendant's DevLAN computer.

Q. Do you recognize this?

A. Yes, I do.

Q. What is it?

A. This is the output of a command that was entered into a terminal session.

Q. What's a command?

A. So, a command would be calling a program to execute on the computer.

Q. And you said a terminal session?

A. Yes.

Q. What is a terminal session?

A. The -- it's a -- it's a specific mode where you are typing in commands, very similar to the old DOS days, where you type something in, you get text back. It is not a GUI interface where you're clicking through.

MR. LAROCHE: Ms. Hurst, can you zoom in on the first three lines that are highlighted at the top, please.

Q. Let's start with the first line. It says root@OSB. What does that mean?

A. That signifies that via SSH you logged in as the root user on the OSB server.

Q. And next to root@OSB, what is VMFS?

A. In this case, it is a directory on the OSB server. It's a folder that's used for VMware.

Q. What about volumes?

A. Again, it's another folder that's just descriptive for the information that's held in it.

Q. And the long number and letters after that?

A. This would have been a unique identifier for a specific VM, I think.

Q. And next to that there's an LS. Do you see that at the end of the line?

A. Yes.

Q. What is LS?

A. LS is a command in Linux to list everything that is in a directory.

Q. And do you see the dash ALTR?

A. Yes, I do.

Q. Do you know what that means?

A. I don't know all of the flags that are on this, but those flags tell LS what information you are looking for.

Q. And what does this command do, LS?

A. It gives you a list of files in a folder.

MR. LAROCHE: Let's zoom out again.

Q. What does the rest of this page reflect?

A. This is the output of LS. It's -- these are the files that were in that folder that was requested.

MR. LAROCHE: Could we go to the next page. And if we can zoom in on the last quarter or so of the page, please.

Q. Before the last line, what are you seeing on this page?

A. A collection of log files.

Q. And why were these log files displayed?

A. They were requested by the LS command.

Q. And do you see the last line of log file that is dash RW 1, root, root and then a 653670 number?

A. Yes.

Q. What is that?

A. So, the -- this is the permissions that are assigned to the file, who has access to this file, as well as the size of the file.

Q. Is this file dated?

A. Yes, it is.

Q. What's the date?

A. The date in this was April 20 at 9:55 p.m.

Q. And do you see that some of the files before that have different dates?

A. Yes.

Q. Why is that?

A. So, it's the date -- I don't know if this is the created or modified date that we're looking at, but their time stamps are slightly different.

MR. LAROCHE: Let's go to the last line of this log file.

A. OK.

Q. There's another root@OSB. Do you see that?

A. Yes.

Q. And at the end, there is an RM VPXA.log? What does RM mean?

A. It deletes a file.

Q. And what is VPXA.log?

A. It is a log file on this system.

MR. LAROCHE: Let's go to the next page, please, and then zoom in on the highlighted text.

Q. What are you seeing here?

A. More deletions of log files.

Q. Is viewing log files an administrative activity or a user activity?

A. Administrator activity.

Q. What privileges are required to do so?

A. You would need access to the location the log files are kept.

Q. Would that be administrative access?

A. Yes.

Q. Did you delete any log files on April 20, 2016?

A. No, I did not.

Q. How long did you act as an administrator of the Atlassian services?

A. I believe about a year and a half. I don't -- I don't know for sure.

Q. How long did you act as an administrator for the ESXi server?

A. Over the entire time we had that ESXi server.

Q. Over any of those times, did you ever delete log files?

A. No, I did not.

Q. Why not?

A. There was no good reason to.

Q. What do you mean by that?

A. Log files are there for a reason. They're to help us identify problems and be able to correct them. They're relatively small in size, so there's no reason to delete them.

MR. LAROCHE: You can pull that down.

Q. I want to switch gears a little bit and I'm going to show you --

MR. LAROCHE: And Ms. Hurst, just for the witness, the parties and the Court.

Q. -- what's been marked as Government Exhibit 801.

MR. LAROCHE: If you could go to the next page, please, for the witness, and the final page.

Q. Do you recognize the handwriting in this document?

A. Yes, I do.

Q. Whose handwriting is it?

A. Josh Schulte's.

Q. How do you recognize that handwriting?

A. I spent a lot of my career trying to understand Josh's handwriting.

MR. LAROCHE: Your Honor, the government offers Exhibit 801 into evidence.

MS. SHROFF: Your Honor, may I have a minute?

THE COURT: Yes.

MS. SHROFF: Your Honor, we object to this document coming in through this witness. The government has to connect it, but this is not the appropriate witness for it to come in.

THE COURT: Mr. Laroche.

MR. LAROCHE: He recognized the document as his handwriting. I think that's sufficient for authentication purposes.

THE COURT: Overruled.

MS. SHROFF: That's not sufficient, your Honor.

THE COURT: The objection's overruled.

MR. LAROCHE: I'm sorry, your Honor. We were going to offer this in evidence.

THE COURT: Received in evidence.

MR. LAROCHE: Thank you.

(Government Exhibit 801 received in evidence)

MR. LAROCHE: Can you please publish that to the jury.

Q. Now, do you have any idea when this document was created?

A. No, I do not.

MR. LAROCHE: Well, I just want to have you look at some portions of the document.

First, at the top, please zoom in on the title.

Q. Can you read that, please?

A. Malware of the Mind.

Q. Do you have any idea what that's referring to?

A. No, I don't.

MR. LAROCHE: We can pull that down.

Please go to the third page and zoom in on the second paragraph, please.

Q. Please take a moment and read that into the record.

A. "Which brings me to my next point. Do you know what my specialty was at the CIA? Do you know what I did for fun? Data hiding and crypto. I designed and wrote software to conceal data in custom-designed file systems contained within the drive's slack space or hidden partitions. I despise data. I split data across files and file systems daily to conceal the crypto. Analysis tools could never detect random or pseudorandom data indicative of potential crypto. I designed and wrote my own crypto. How better to fool buffoons like forensic examiners and the FBI than to have custom software that doesn't fit into their two-week class where they became forensic experts. Make no mistake. I am an expert in data hiding and cryptography with thousands of hours of experience and among the top specialists in the world (or was). I mean, how many?"

Q. You talked earlier about trade craft?

A. Yes.

Q. Do you see any trade craft in this paragraph?

MS. SHROFF: Objection.

A. Yes.

THE COURT: Overruled.

Q. What trade craft is contained in this paragraph?

A. His discussion about crypto, hiding data in, like, slack space and hidden partitions. I believe that covers what was in here.

Q. Why is that considered trade craft?

A. These are techniques that we use to hide data, exactly as was stated in here.

Q. Is that trade craft classified?

A. Yes, it would be.

Q. Why?

A. In the giving -- acknowledging that this was a technique that we used would help an adversary detect us on the system.

Q. Other than testifying today, have you ever spoken publicly about this trade craft?

A. No, I have not.

Q. Why not?

A. It was classified information, and doing so would damage our potential operations.

MR. LAROCHE: You can pull that down. Thank you.

Ms. Hurst, can you please publish just to the Court, witness and parties Government Exhibit 806. And just go through the next few pages.

Q. Mr. Weber, do you recognize the handwriting in this document?

A. Yes, I do.

Q. Whose handwriting is it?

A. Josh Schulte's.

MR. LAROCHE: Your Honor, the government offers 806 into evidence.

MS. SHROFF: Your Honor, we have the same objection.

THE COURT: OK. Same ruling. Overruled.

Received in evidence.

MR. LAROCHE: Thank you, your Honor.

(Government Exhibit 806 received in evidence)

MR. LAROCHE: If we could go to the last page and then publish it for the jury. And please just zoom in on the top left date.

Q. Mr. Weber, can you please read that?

A. 7/14/18, Saturday.

MR. LAROCHE: And if we can zoom out and zoom in on the text on the right.

Q. Can you please read that text, starting at the top?

A. "New attack plan.

"(1) FBI not the only agency against Trump. CIA too.

"(a) leak documents to make Trump look bad

"(b) sell documents to make money.

"(2) political dissent." I don't, I don't know if I can read that word.

"(3) incompetence at the CIA, government agencies.

"(4) if I were Russia, I would blank

"(a) attack judiciary

"(b) U.S. destroy itself."

MR. LAROCHE: Thank you. We can pull that down.

Ms. Hurst, can you please show the witness, the parties and the Court Government Exhibit 809 and just flip through a few of the pages on this document for the witness, please.

Q. Do you recognize this document?

A. Yes, I do.

Q. Do you recognize the handwriting in this document?

A. Yes, I do.

Q. Whose handwriting is it?

A. Josh Schulte's.

MR. LAROCHE: The government offers Government Exhibit 809 into evidence.

MS. SHROFF: Same objection, your Honor.

THE COURT: OK. 809's received in evidence.

(Government Exhibit 809 received in evidence)

MR. LAROCHE: Ms. Hurst, can you please go to page 9 and then publish it for the jury.

Ms. Hurst, can you please zoom in on the line that starts "Twitter," in the middle of the page.

Q. Can you read that, Mr. Weber?

A. "Twitter: Free Jason Bourne."

Q. Who is Jason Bourne?

A. Jason Bourne was a fictional character in the Jason Bourne movies.

Q. And what type of character was he?

A. He was a superagent for the CIA.

MR. LAROCHE: If we can zoom out, please.

Ms. Hurst, can you focus in on the next four lines before free Jason Bourne -- or four lines below. Sorry.

Q. Can you read that, please?

A. "The @Department of Justice arrested the wrong man for Vault 7. I personally know exactly what happened, as do many others. Why are they covering it up?" And then "must be" or "meet."

The bottom portion's cut off a little bit there.

MR. LAROCHE: Let's look at the remaining portion of that page.

Q. Starting with the line that says "meet," in the middle there, by your name --

A. "Meet the CIA's stir sack or struck Jeremy Weber and Karen. You can find his info in the Ashley Madison dump at the CIA. Set up Joshua Schulte. Jeremy Weber hacked Atlassian's Crowd and when Schulte -- the admin found out, Karen issued him a memo/letter of" -- the handwriting's difficult -- "a letter of warning for self-granting admin privileges. The system administrator self-granting admin privileges. Hmm. Right over the FBI's head too. Or was it?"

Q. Just stop there for a second.

One of the things that's written by the defendant here is Jeremy Weber and Karen set up Joshua Schulte. Did you set up Joshua Schulte?

A. No, I did not.

Q. The defendant then writes, "Jeremy Weber hacked Atlassian's Crowd." Do you have any idea what he's referring to there?

A. No.

Q. Did you ever hack Atlassian's Crowd?

A. No, I did not.

Q. Please read the bottom portion of this page.

A. "Schulte is the scapegoat because he routinely reported security issues at the CIA, including infrastructure branches, abysmal" -- management, maybe. I don't know the last word there.

Q. Did the defendant routinely report security issues at the CIA?

A. No, he did not.

MR. LAROCHE: Can we go to the next, page, please, and just focus in on the top left quarter of this page.

A. "At USG, just to authenticate me first, the @CIA was involved in blank. The code for initially planned cyber operation is in Vault 7. Tool described in vendor report is, in fact, Bartender, CIA tool set for operators to configure for deployment."

Q. Are you familiar with Bartender?

A. Yes, I am.

Q. What is Bartender?

A. It is a tool that I worked on for an extent -- the majority of my career in OSB.

Q. Generally speaking, what does that tool do?

A. The tool was meant to collect files from a computer via thumb drive that an operator had access to.

Q. The defendant wrote that Bartender was described in a vendor report?

A. Yes.

Q. Is that right?

A. Yes.

Q. Did the vendor report attribute that tool to the CIA?

A. No, it did not.

Q. Has the CIA ever acknowledged that that's a CIA tool?

A. No, it did not.

Q. Why not?

A. The attribution, especially in this scenario, would be very concerning because operators were the ones that would start this tool, and if it was caught, attribution could lead to the capture of a CIA officer.

Q. Other than testifying today, have you ever discussed Bartender publicly?

A. No, I have not.

Q. Why not?

A. It was classified information. Discussing it would put CIA officers' lives at risk.

MR. LAROCHE: You can pull that down.

Q. Early in your testimony today, you talked about the March 7 leak?

A. Yes.

Q. I want to turn your attention back to that.

A. OK.

Q. One of the things you said was that the first leak, on March 7, 2017, contained Confluence data, is that right?

A. That's correct.

Q. And that's Confluence data from DevLAN?

A. Yes.

Q. How much of Confluence was disclosed on March 7, 2017?

A. Everything up until a certain date.

Q. In what locations on DevLAN was all of the Confluence data available?

A. It would have either been in the Confluence VM or in the backups.

Q. I want to talk about a few documents that were disclosed by WikiLeaks from that first initial leak.

A. OK.

MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 6 and zoom in on the text.

Q. Showing you a portion of the directory from the March 7 leak, do you recognize that?

A. Yes, I do.

Q. And what is this? What are these lines?

A. So, the first line, data transfer modules, was -- this was a page on Confluence. Everything below that is subpages to that that talked about specific ways that we would store data for transfer.

Q. And can you read the third line?

A. Yes. "Transferring data using NTFS alternate data streams, DG NTFS ADS BK Brutal Kangaroo."

MR. LAROCHE: Let's go to Government Exhibit 6-1, please. If we could just zoom in on the middle, starting "transferring data," including the banner.

Q. What is this page showing?

A. This page is a description of this specific technique.

Q. And does that connect to the last exhibit we saw in any way?

A. Yes, it's -- if you had clicked that link, it would take you to this page.

Q. And you said a specific technique. What were you referring to there?

A. I mentioned earlier that EDG does eight things a thousand different ways. One of those eight things is data -- transferring data. This technique is a way of -- one of the many ways that we would store data and transfer it between a target machine to a CIA infrastructure.

Q. Just focusing on the parentheses there, it starts DTN and there's some more letters. Do those letters have any significance?

A. Yes, they do.

Q. What significance?

A. The DT is an abbreviation for data transfer. NTFS ADS is for NTFS alternate data streams, which is the technique, the specific technique that's being used here. And BK is letting other people know that this was originally designed for Brutal Kangaroo.

Q. What is Brutal Kangaroo?

A. Brutal Kangaroo was a tool suite created by Josh Schulte.

Q. And then underneath this title, there's a secret/noforn banner?

A. Yes.

Q. Just remind us what that is.

A. The classification of this document was secret and should not be shared with any foreigners.

Q. Was this one of the documents that was obtained from Confluence?

A. Yes, it was.

Q. Was it common to post classification banners on Confluence?

A. Yes, usually it was. It wasn't a universal -- it wasn't a universal thing, but it was something we often did.

Q. And why?

A. It helped so that we knew what type of page we are seeing.

MR. LAROCHE: We can zoom out again.

And then if we could go to Government Exhibit 6-2.

Q. Showing you another version of the previous exhibit, do you see the same title there?

A. Yes.

MR. LAROCHE: If we could go down to page 2 and then zoom in on the notes.

Q. Can you summarize what these notes are showing?

A. This explains how to use -- how to use the technique as well as what information is in the technique so that you could -- this is meant to help somebody implement this.

Q. You've talked about attribution before, attributing tools to the CIA?

A. Yes.

Q. What, if any, impact would the disclosure of this information have on attributing a tool to the CIA?

A. This is a pretty significant clue.

Q. Why?

A. It tells exactly how data at rest is stored. So if somebody was doing a forensic review and saw a structure like this as well as these types of commands, they now have something that says this was a CIA tool.

MR. LAROCHE: We can pull that down.

Ms. Hurst, please publish Government Exhibit 11-2.

Q. What is this?

A. This is a, just a help page that was on Confluence.

MR. LAROCHE: And if we can just zoom in on the "wait" and the banner for a second.

Q. Do you recognize this page at all?

A. Yes, I do.

Q. And why do you recognize it?

A. It was something that was on our Confluence and was something that I would have read at some point.

MR. LAROCHE: And if we can go back out a second, just to the wider one, and then zoom in on the first two paragraphs.

Q. Summarize what these paragraphs are describing.

A. So, the first paragraph is just talking about some history of a previous, you know, previous deployment of a tool.

And the second part is talking about, talking about attempting to overwrite a file that was written to obfuscate our involvement and finding out that that file wasn't correctly overwritten.

Q. Have you ever talked about this type of information publicly before?

A. No, I have not.

Q. Why not?

A. This is all techniques and, in this scenario, would have been a specific operation that we were supporting.

MR. LAROCHE: If we can go to Government Exhibit 15.

Q. Earlier today we showed you a user guide for Brutal Kangaroo. Do you recall that?

A. Yes, I do.

Q. What part of the WikiLeaks disclosure did that document come from?

A. I don't remember if that document was in Confluence or Stash or both.

Q. Do you remember subsequent disclosures from Stash?

A. Yes.

Q. Is this one of the documents, Government Exhibit 15, that came from Stash?

A. Yes.

Q. And what is this document?

A. This is a slide deck that was created for the delivery of Emotional Simian version 2.0.

Q. Are you familiar with it?

A. Yes.

Q. How are you familiar with it?

A. I was the primary author.

Q. Generally speaking, what is Emotional Simian?

A. Emotional Simian was a thumb drive-collection tool that was designed for a scenario where the owner of a thumb drive was unwitting to the fact that he was spreading malware by moving the thumb drive between machines.

Q. What do you mean by unwitting?

A. The target did not know that they were a CIA target, nor did they know that there was a CIA operation occurring.

MR. LAROCHE: Let's go to page 3.

Q. We're now on a page that's titled requirements.

A. Yes.

Q. What is a requirements page?

A. Requirements -- this is a very high-level discussion of what the tool is supposed to do.

Q. And what was this tool supposed to do?

A. In this case, provide access to downstream machines that would otherwise be inaccessible via thumb drives inserted by unwitting users.

Q. You said downstream machines?

A. Yes.

Q. What does that mean?

A. This is a term that we used in the agency. You're -- you would have a point of presence on the network somewhere, access to a computer. Downstream machines are further into the network that we don't necessarily have access to yet.

MR. LAROCHE: Let's go to the next page, please.

Q. And this page is titled concept of operations?

A. Correct.

Q. What is a concept of operations?

A. This is a high-level description of how we imagine the deployment of the tool would go.

Q. And do you recognize the page?

A. Yes.

Q. How do you recognize it?

A. I created it.

Q. If we could just look at the diagram there in the middle --

A. OK.

Q. -- can you summarize what that diagram is telling us?

A. This takes you through the steps that the deployment of this tool would go through. It would start on a configuration machine, something that the agency owned, to the primary host, which is that initial foothold that I had mentioned earlier, and then, via a USB drive, infect secondary targets downstream.

MR. LAROCHE: If we can go to the next page, page 5.

Q. This is titled capabilities and limitations?

A. Yes.

Q. What is this page showing?

A. So, this is explaining -- like, there's no tool that does everything. So this was explaining what the tool did and didn't do.

Q. Other than testifying today, have you ever spoken publicly about Emotional Simian?

A. No.

Q. Why not?

A. There, again, it would expose our methods and allow for the detection of this tool.

MR. LAROCHE: We can pull that down, please.

Q. Focusing you again on March 7, 2017, just to orient us a bit, prior to that, what was your typical workday like?

A. Nine to five. You know, some days longer than others, but it was traditionally an eight-hour day.

Q. Did that change after the leak?

A. Yes, it did.

Q. How did it change?

A. The most noticeable impact was in that first week I was assigned to lead a team to assess what was in the leak and what the damage was. That was -- for that week I often would work until about 2 a.m., go home for a few hours and then be back at work around 6 a.m. to make sure that I could brief -- brief senior leadership about the status of our work.

Q. Why were you working those long hours?

A. We were -- we were in damage mode, like the house was burning down, and we were trying to figure out what was going on.

Q. You said you were working on a team?

A. Yes.

Q. How many people were working on that team with you?

A. I think it was about ten.

We took one or two of the most senior developers in each of the branches in AED, and they were assigned to me to make assessments of what was in the leak.

Q. What were some of the things you were doing on that team?

A. There were three major focuses.

One was understanding what all had leaked out.

The second was looking for the biggest, like, "oh, crap" disclosures, that if we saw this we need to inform people immediately, because there's significant problems.

And third, we were looking for any information -- in addition to the leak, WikiLeaks published an editorial. We were reading through that editorial and seeing if they referenced any information that wasn't in the leak to see if there was any proof that they had additional information.

Q. Now, at the time of the leak, you had been at the agency for how long?

A. I think close to seven years at that point.

Q. And during that time, you'd worked exclusively as a developer developing cyber tools?

A. No.

Q. What else did you do?

A. A few months prior to the leak, I had become a branch chief for one of the other branches in the division.

Q. Did that branch also develop cyber tools?

A. Yes, it did.

Q. During that time that you were at the CIA, what impact, if any, did the public disclosure by WikiLeaks have on your past work?

A. So, the public disclosure of my past work pretty much meant all of that work was now no longer operationally useable. It was dead.

Q. Why?

A. The risk of attribution to the CIA as well as the amount of information that adversaries would have for detecting our operations was too high, and we needed to rewrite that work.

MR. LAROCHE: No further questions, your Honor.

THE COURT: Ms. Shroff.

CROSS-EXAMINATION

BY MS. SHROFF:

Q. Good afternoon, Mr. Weber.

A. Good afternoon.

Q. Mr. Weber, you testified that you've worked at the CIA for about seven years, is that correct?

A. No, that's not correct.

Q. I'm sorry. Could you correct me then?

A. It was close to ten years.

Q. You've been at the CIA for close to ten years?

A. That's correct.

Q. And I have it right, do I not, that you started at the CIA before Mr. Schulte did? Correct?

A. I started full time before Joshua became a full-time officer. He did internship tours shortly before I started full time.

Q. So when you and Mr. Schulte worked together, were you both essentially at the same level?

A. I was a little bit ahead of him in grade, but we were close.

Q. And what would your title be at that time?

A. Developer would be the official title.

Q. And Mr. Schulte was also a developer, correct?

A. Yes.

Q. And you worked, both of you worked in the same group. Do I have the nomenclature correct?

A. Yes, same group.

Q. And what was that group? Remind me, please.

A. Engineering Development Group.

Q. And at that time, how many people worked in EDG?

A. In EDG, maybe 200. I don't know. I don't know the number.

(Continued on next page)

Q. The supervisor for you and Mr. Schulte, your immediate supervisor, was whom?

A. During what time?

Q. Well, let's stick with 2015 and 2016, the same time frame that Mr. Laroche covered.

A. Then that would have been Sean.

Q. So, you were never Mr. Schulte's boss, correct?

A. No. Not in an official capacity.

Q. There's only one capacity in which you can be someone's boss, right?

A. No, that's not correct.

Q. So, the CIA had such a loosey-goosey structure that you could be somebody's unofficial boss?

A. There are two types of leadership positions in the agency.

Q. So did you -- are you saying there are two types of formal leadership positions in the agency?

A. One is --

Q. No, no. Could you answer that question first?

A. Could you repeat it?

Q. Sure. I just wanted to make sure if I understood you correctly that there are two types of leadership positions.

What does that mean, by the way, "leadership position"?

A. Leadership position has a very broad, broad definition.

Q. So, I don't understand what it means. I have a boss. I don't know what a leadership thing is. Can you explain that?

A. So the agency, there's two types of leadership in the agency. Your official, like, leadership, the branch chiefs, things of that nature, have what we refer to as -- you have a responsibility to officially review an officer's work, and document that for the record.

There are a significant additional amount of leadership positions like team leads or project leads that you might, you might provide feedback to the branch chief, but you would not have an official say in the documentation of like how good or bad an officer was doing.

Q. Okay. But when you were assigned to be a team lead or a project lead -- not just you, in particular, but a person -- somebody assigns an individual to be a team lead, correct?

A. Occasionally. Sometimes it is just a natural formation. It depends.

Q. Okay. Let's talk about a project lead, or is that the same thing?

A. A project lead is one of the categories, yes.

Q. So when there is a project or a tool, a group of people work on it in the CIA; is that how it works?

A. Sometimes. Sometimes people will work on things by themselves, but yes.

Q. All right. so let's talk about when there is a group working on it, okay?

A. Yes.

Q. And when there is a group working on it, you said that there is either a natural team leader, or some boss assigned somebody and says "you are the team leader." Correct?

A. Yes.

Q. And if somebody assigns a team leader, everybody knows that that team leader is assigned, correct?

A. Yes.

Q. Okay. And if it's just somebody who assumes a leadership, the other people don't have to follow that leadership. They can say, well, you're not the the team leader. Correct?

A. No, that is not correct.

Q. So anybody can just become a team leader on a project?

A. We all had ownership of projects. And whoever owned a project would be the natural leader of it.

Q. Right. But I'm trying to figure out this natural leader concept. All I'm trying to figure out is if you didn't like your natural leader, could you say, hey, you're not my natural leader on a project or not?

A. You could say you're not my leader and no longer work on the project.

Q. Or you could go to Sean and say, hey, this guy's not my natural leader, correct?

A. That's correct.

Q. And then Sean would figure it out, correct?

A. Yes.

Q. Right. And in your particular unit, Sean was the person who would generally figure things out, right?

A. At the time we're talking about, yes.

Q. We're only going to talk about that time, so you don't have to worry about that. Okay? If I pick a different time period, I'll tell you, okay?

A. All right.

Q. So you testified about this time period and you said basically EDG was a -- correct me if I'm wrong because I don't have a transcript in front of me. Was a friendly, collegial place, correct?

A. Yes.

Q. And is it fair to say that most of the people who worked in EDG were men, or is that not correct? I don't know.

A. I can speak more to AED.

Q. I'm only talking about the group you worked with Mr. Schulte, 2015 to 2016.

A. AED was below that group.

Q. Right.

A. So, AED, that's a fair statement. EDG as a whole, I don't know. I don't know what the layout would have been.

Q. Okay. Let's just focus on your subgroup then. Mostly men you would say?

A. It was predominantly male.

Q. And about how many -- you remember the diagram that Ms. Hurst showed you of the ninth floor. If you could just pull it back up, please.

While she's pulling it up, you basically showed it was cubicles in which all of you sat, correct?

A. Yes, that is correct.

Q. And you sat somewhere next to Amol, correct?

A. That is correct.

Q. And somewhere next to Mr. Schulte?

A. That is correct.

Q. And then who was the person in the fourth cubicle?

A. Like at an angle from me?

Q. Yeah.

A. That would have been Frank.

Q. Frank?

A. Yes.

Q. You testified basically that it was a collegial environment?

A. We were friendly with each other, yes.

Q. Friendly with each other. All right. Part of this friendliness included people playing with each other with Nerf guns?

A. Some developers did that.

Q. And they weren't like these teeny little Nerf guns, right? They were like real serious investment of big plastic Nerf guns; is that correct?

A. There were all manners, but yes, some of them were as you described.

Q. How many Nerf guns do you think all together were in this little cubicle area? Four, six, 10, 12?

A. In our cubicle area, if I recall correctly, only Josh and one other person had Nerf guns.

Q. And then in the broader cubicle area, other people had Nerf guns?

A. Across the floor, yes.

Q. Okay. And they shot Nerf -- whatever comes out, I don't know, I don't play with Nerf guns. But whatever it is that come out of the Nerf guns, they shot at each other?

A. Occasionally.

Q. It was more than occasionally, right?

A. I didn't take part in it, so I don't know.

Q. Amol took part in it in terms of being annoyed by it, correct?

A. I don't remember actually.

Q. Really?

A. Yes.

Q. You don't remember Amol being annoyed by Mr. Schulte shooting Nerf guns at him?

A. I remember Amol being annoyed by Mr. Schulte on occasion.

Q. That we know.

A. I don't specifically -- if he ever expressed it about the Nerf guns.

Q. Okay. Do you recall Amol being annoyed at the Nerf gun darts coming at him, and he would take the darts and throw them behind his own desk?

A. Actually, yes. I do remember that now.

Q. Okay. Do you recall Amol or Mr. Schulte taking stuff from each other's desks and hiding it behind each other's back?

A. No, I do not.

Q. Do you recall a general sense of people teasing each other about habits and appearances?

A. Habits, yes. Appearances, typically no.

Q. You don't remember Amol calling him a bald asshole?

A. I do recall that, yes.

Q. He actually used to call him bald asshole, right?

A. Yes.

Q. And there was a gentleman in that unit that had some kind of unfortunate autoimmune disease. Do you recall that human being? The person -- I just, I don't want to personally out someone's health issues.

A. No, I don't remember an autoimmune disease, no.

Q. Do you remember Amol telling somebody that he was going to drop dead anyway, and stop complaining about the pain he was feeling?

A. No, I do not recall that.

Q. You don't recall that. Do you remember being asked about Amol saying that your wife's investment in her work-related 401(k) was a financially stupid thing to do?

A. No.

Q. Do you remember being interviewed on video about this particular allegation and saying to that individual --

A. The allegation that you're referencing is incorrect. Like --

Q. Why don't you tell us what the allegation was.

A. The allegation was that my wife was dumb. And that a decision she made was dumb. I remember referencing an allegation where Josh said that my wife was dumb.

Q. Okay. But Amol did call your wife's decision to invest in a particular investment dumb, correct?

A. Yes.

Q. And he told you that he thought your wife's decision was dumb. Correct?

A. Yes.

Q. And you replied, "Better to have a dumb decision and a happy wife. I can live with that every single time," correct?

A. Very much so.

Q. Make sure you tell my husband that.

So, had Mr. Schulte just written that complaint more carefully, you would have answered the complaint differently as you did during your interview, correct?

A. There is a wide difference in the allegation that he made and what actually happened, so, if he had correctly stated what had happened, I would have answered differently, correct.

Q. And it's fair to say that by the time these allegations were discussed with you, you had long stopped liking Mr. Schulte, right?

A. I can't remember -- yes, I think that is a fair statement.

Q. Now, Mr. Schulte was friends with people in his group and friends with people who worked at the CIA, correct?

A. Yes.

Q. One of those friends was a man named Michael; is that correct?

A. That's correct.

Q. And you knew Michael as well, correct?

A. Yes.

Q. And was he part of your group or was he part of a separate group?

A. The Michael that was his friend was in our branch.

Q. It was in your branch, right?

A. Yes.

Q. And Michael and Mr. Schulte also fought, correct?

A. There was only one scenario that I recall of a fight between the two of them.

Q. Right. When that fight occurred, the person who gossipped the most about that fight was in fact Amol, correct?

A. I don't know.

Q. You don't remember Amol sending texts to everyone saying, hey, you would not believe what happened between Michael and Josh?

A. No.

Q. He didn't send you that text?

A. I don't believe so.

Q. Okay. Suffice it to say that the saga between Amol and Josh went on for quite some time, right?

A. I'm sorry. Can you repeat the question?

Q. Is it fair to say that the saga between Amol and Josh went on for quite some time?

A. Yes. As I stated earlier, they didn't get along and from the getgo. And it depends when you want to define a saga beginning.

Q. Okay. Well there came a point when you defined when the saga began, right?

A. Yes.

Q. Okay. And you said that, for you at least, the breaking point was that you thought Mr. Schulte had lied about Amol's behavior towards him?

A. Yes.

Q. And you were aware that Mr. Schulte was so upset by Amol's behavior that he went to court, correct?

A. I was aware that he went to court. I don't know why he went to court.

Q. He didn't tell you he was upset?

A. I was not talking to him at this point.

Q. Okay. So, by then you had stopped talking to him?

A. Yes.

Q. Okay. But you were talking to Amol?

A. Yes.

Q. And Amol had gone to court with you?

A. Amol, I don't know -- at one point I went to court with Amol. I don't know Amol's court appearances prior to that.

Q. Okay. So Amol told you the version of what Mr. Schulte was doing?

A. Yes.

Q. And you believed Amol?

A. I saw what Amol had as well as the -- I read Mr. Schulte's allegations.

Q. But you weren't talking to him?

A. No.

Q. So you heard what Amol said, and then you continued to side with Amol?

A. Yes.

Q. Okay. Now, let me just move just very briefly for a second from that to how the CIA maintained, as you called it, physical security. Right.

A. Okay.

Q. So you testified that to get into the CIA, physical location, right, you had to have a badge, right?

A. That is the way that I would have accessed it. I had a badge. Other people might not and would present like a driver's license, and if they were on an access list, they could, you know, access the facility.

Q. Okay. So when you access the CIA facility, do you drive into like a big compound and then go to a building?

A. After you present your badge the first time, yes.

Q. Right. And then there's like a whole gigantic parking lot or something like that where people park their cars?

A. Yes.

Q. Is there more than one physical building structure on that lot?

A. Yes.

Q. How many physical structures are there?

A. The, at that time, I believe there was two. I don't know. I don't know the status.

Q. Now, to go from one physical structure to another physical structure, you didn't have to go through any additional driving or security, correct?

A. Once you were inside the building, the two physical structures I referenced were connected by a tunnel.

Q. So, once you got inside the building, you had CIA employees inside the building, correct?

A. Yes.

Q. You had people who contracted with the CIA and were contractors, correct?

A. Yes.

Q. You had support staff and other staff who were part of the CIA's workforce, correct?

A. That would fall into the one of the first two categories you described.

Q. All told, how many people worked in that big area?

A. I have no idea the number. It was large.

Q. It was large, right?

A. Yes. It was a nine-floor building.

Q. So you would say over 1,000?

A. I don't know.

Q. You don't know. When you went from one building to another building, you could carry with you documents, correct?

A. You were not leaving the secure portion of the facility, so yes, that is correct.

Q. You could carry with you computers, correct?

A. Yes, that is correct.

Q. You could carry with you laptops, correct?

A. Yes.

Q. In fact, there were times when somebody moved from one building to another, just physically carried their stuff with them, correct?

A. Yes. We were authorized to transport classified information.

Q. Okay. When you worked at the CIA with Mr. Schulte, you never saw Mr. Schulte walk off that garage or compound with a hard drive, did you?

A. No.

Q. Did you ever see him walk off with a disc, did you?

A. No.

Q. How about a thumb drive? Did you see him walk off with a thumb drive?

A. No.

Q. How about a computer? Did you see him walk off with a computer?

A. No.

Q. When he worked at the CIA with you, did you ever see him use a cell phone inside the facility?

A. No.

Q. And it's fair to say you would never do such a thing, right?

A. Yes.

Q. Let's talk about systems security. Right. Because you testified on direct with Mr. Laroche that you thought that the DevLAN system was secure, right?

A. Yes.

Q. Is that still your testimony now?

A. Yes.

Q. Correct me if I'm wrong on any one of these, okay?

CCI work product properly resided on the DevLAN network; is that correct?

A. I'm sorry. CCI work product?

Q. Right.

A. Properly resided on the network. Yes?

I don't know if I fully understand the question. Like, what's a work product?

Q. It's not a trick. I'm just asking if the work that group did was on the DevLAN network?

A. So, CCI is the largest portion of the umbrella. There was a subset of CCI's work product, the stuff that was made by AED, that would have been on the network. Maybe some other stuff from other groups, but it was focused on EDG's product. Not necessarily CCI's.

Q. Is it fair to say that CCI --

Let me take one step back.

What is CIMC; do you know?

A. It is the group that is specifically focused on investigating counterintelligence and counterespionage.

Q. You've told us about every other acronym. Tell us what CIMC stands for.

A. CIMC is the Counter Intelligence Mission Center.

Q. And is it fair to say that the CCI did not work with CIMC to properly develop or deploy user activity monitoring?

A. That was outside my scope.

Q. Okay. Would you agree with me that the system lacked robust server audit capability?

A. I don't know what type of auditing was on the servers.

Q. But you testified on direct that the servers were secure, right?

A. I can talk to the Atlassian products. I can't talk to every server that was on DevLAN.

Q. How about the ESXi server?

A. The OSB ESXi server, it had some level of auditing that we felt there was a need for.

Q. You have to say that again.

A. The OSB ESXi server we had the default auditing enabled. So, we felt that was good enough for the needs for that server.

Q. Good enough?

A. Yes.

Q. What does that mean, "good enough"?

A. There's different, different levels of information. As I had stated, most of what was on the OSB server was, it was non-production data. It was test VMs and things like that.

Q. So you didn't think it was that secure or that secret, so it didn't have to have a robust server audit capability?

A. I -- we set it up to defend what we -- we set it up to a point where I feel it was good enough.

Q. I'm sorry. Is that the place from which all of this stuff was stolen?

A. I don't know where all of this stuff was stolen from.

Q. Oh. Okay. All right. Let's try the next one.

Is it fair to say that the cyber weapons were not compartmented?

A. Generally correct.

Q. What does that even mean? Can you help me out here?

A. There were cases where some of our cyber capabilities would have been compartmented.

Q. What does that mean though? I'm sorry.

A. I apologize. Compartment is very strict handling for specific scenarios. Very limited need-to-know access.

Q. Right. And the cyber weapon is what?

A. Sorry, say that again?

Q. What's a cyber weapon?

A. A cyber weapon would be a potential term for the type of capabilities we make.

Q. What does that mean, "type of capabilities we make"?

A. We made cyber tools.

Q. Right.

A. If you want to refer to them as weapons, I would probably disagree with that terminology. But, other people might agree with it.

Q. Could you just give me one second?

A. Sure.

(Counsel conferring)

Q. Let me just stick to my question, okay. I got distracted for a minute. I apologize.

By cyber weapon you mean the tools that your unit created, right?

A. Like I said, it could be a definition. It's not how I would describe them.

Q. Well, let's just go with what you would describe it. You would call it some kind of malware, right, you said?

A. That would be an industry term I think is accurate.

Q. By malware, you basically mean it's something that the United States creates so they can go spy on a foreign government, correct?

A. That's one of the scenarios that we created it for.

Q. Right. And basically, when we speak like this, like it's the scenario we created for, just to simplify it because we don't all work at the CIA.

A. Yes.

Q. Right. So, you create a tool because you want to know what some other countries, say Iran or France or Germany or some other country, is up to, correct?

A. Without identifying specific countries, that is a correct statement.

Q. So, the people who develop these tools, they make up a tool so that it can be used to get information from a foreign country that we want. But we don't want anybody to know we're doing it, so we try and hide it.

That's what all of these people are doing at EDG?

A. Yes.

Q. That is what you call a cyber tool, a cyber weapon, a malware tool, all of these fancy words are just for what I described, correct?

A. Yes.

Q. Okay. Of course, nobody wants it to be tracked back to us, because then nobody would talk to us, correct?

A. That is correct.

Q. Is it fair to say that the users on these servers that we have, and that you talked about, shared system administrative level passwords?

A. For some servers.

Q. Isn't that like a bad thing to do?

A. Depends on the scenario.

Q. Can you think of any good reason, from a security perspective, I'm not talking about collaboration and getting things done fast, which is why I think this was done. I'm just talking from a security perspective, can you think of any reason you would ever have users share a system at an administrative level where the passwords are shared?

A. Yes.

Q. From a security point of view?

A. Yes.

Q. Tell us why.

A. Your typical scenario would tend to be a backup account in case, in case your connection with Active Directory or something like that broke.

Q. If one person's connection broke, that means they could use somebody's else's password?

A. It was supposed to be a backup password for in case there was no longer the traditional ways of logging in.

Q. Okay. So if you, for example, were logged out, or locked out, you could go to this shared system admin level, because at one point you were admin, and you could take one of those passwords and log on in, correct?

A. Yes.

Q. Okay. And could you just take any password?

A. No.

Q. So which password would you pick from all of these passwords?

A. What passwords are you referring to?

Q. These shared system admin level password.

A. The ones that we discussed earlier?

Q. Yeah.

A. I don't know. What am I trying to do?

Q. All I'm asking you is, it isn't the best way to keep a network safe. Correct?

A. It is -- you want to ensure that people are logging in with a unique user name and password as much as possible.

Q. Right. This defeats that, correct?

A. This would circumvent that.

Q. I'm sorry, he coughed. I couldn't hear you.

A. This would circumvent that.

Q. Right. There was another problem with the system in the sense that there was no effective removable media control, correct?

A. I can't comment to that.

Q. Well, let's see if we can try. You testified with Mr. Laroche here that you were part of this recovery effort after the leak, correct?

A. Yes.

Q. When was the first leak in your mind?

A. March 7.

Q. March 7. And when the March 7 leak came, did anybody at the CIA say, hey, is this about it or is there more to come?

A. I -- I was not part of any conversations like that. It was not my focus at the time.

Q. It was not your focus to see what else could be coming down the turnpike, considering this was like the CIA's most precious hacking tools?

A. My focus was on assessing what was in Confluence and what information we could take from Confluence.

Q. Okay. So when you first discovered that this had been put on WikiLeaks, how long did it take, not you personally -- or let's start with you personally.

How long did it take you to figure out that the stuff was like a year old?

A. It would have been during that first week.

Q. It took a whole week to figure out it was a year old?

A. It wasn't something we were specifically trying to figure out at the time.

Q. How many people were on your team?

A. Are you referencing the team during that first week?

Q. Yeah.

A. About 10 people.

Q. 10 people were on your team. Right?

A. Give or take.

Q. How many teams were there, all told?

A. During that first week, I think there might have been two teams. I don't recall.

Q. On these two teams, it took a whole week to figure out that the information you guys were talking about was a year old.

A. We were not looking for that information.

Q. You were trying to assess damage, right?

A. Yes.

Q. You were trying to assess damage of a leak, correct?

A. Yes.

Q. You wanted to know what was leaked, correct?

A. Yes.

Q. And you wanted to know if that leak was going to hurt, correct?

A. Yes.

Q. So the first thing you want to know is what is leaked, correct?

A. What was leaked, yes.

Q. Right. What was leaked. And how recent is the information. Right?

A. No.

Q. You didn't want to know how recent the information was?

A. I didn't necessarily care.

Q. You didn't care if the most recent tool had been leaked to find out how recent the leak was?

A. I cared about what information was leaked. Not the date of that information.

Q. Right. So when you were trying to figure out what information was leaked, you learned a week later that the information that was leaked was about a year old.

A. I learned during that first week.

MS. SHROFF: Would this be a good place to stop?

THE COURT: I was just going to ask you if this was a convenient place to break.

MS. SHROFF: This is a good place to break.

THE COURT: We are going to break now. And we'll resume at 9 o'clock tomorrow morning.

Please remember my instructions. Don't do any independent research, don't talk about the case. If you see anything in the newspaper, hear anything on the radio, ignore it. You've got to make up your minds when the case goes to you, it's in your hands. You have to consider only the evidence that is brought out in this courtroom, and nothing else.

So, safe home tonight. See you tomorrow morning at 9 o'clock. We'll have coffee and tea for you at 8:30.

Thanks very much.

(Jury excused)

THE COURT: You're on cross-examination so don't talk to the government's attorneys.

THE WITNESS: Understood.

THE COURT: See you tomorrow morning at 9 o'clock.

MR. LAROCHE: Thank you, your Honor.

(Adjourned to February 6, 2020, at 9:00 a.m.)

INDEX OF EXAMINATION

Examination of: Page

JEREMY WEBER

GOVERNMENT EXHIBITS

Exhibit No. Received