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 11, 2020
9:15 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
Matthew Mullery, CISOs, Department of Justice

(In open court; jury present)

THE COURT: Good morning. All right, Mr. Denton.

You're still under oath.

THE WITNESS: Yes.

MR. DENTON: Thank you, your Honor.

DAVID,

called as a witness by the Government,

having been previously sworn, testified as follows:

DIRECT EXAMINATION (Continued)

BY MR. DENTON:

Q. Good morning, sir.

A. Good morning.

Q. I want to pick up where we left off yesterday with some of the events of April 20, 2016.

MR. DENTON: Ms. Hurst, can we bring up Government Exhibit 1069, please.

Q. I just want to go over the times that some of these things happened for a second. Do you remember taking a look at this e-mail about the infrastructure changes yesterday?

A. Yes.

Q. What time was that e-mail sent?

A. The e-mail was sent April 20, at 15:58, almost 4 o'clock p.m.

Q. Do you see next to that where it says GMT minus 04?

A. Yes.

Q. What does that indicate?
A. From Greenwich Mean Time is four hours less than Greenwich Mean Time, which would be Eastern Standard Time.
MR. DENTON: So, if we could then go, Ms. Hurst, to Government Exhibit 1203-25.
Q. Do you remember taking a look at this yesterday, sir?
A. I do.
Q. And the top line that's highlighted in black there that ends in initiated lazy snapshot BKUP?
A. Yes.
Q. What's the date and time of that entry?
A. The date and time is April 20, 2016, at 21:30 Zulu, Greenwich.
Q. And what does that translate to in local time?
A. That is four hours less. So, that would be -- it would be about 5:30 p.m.
MR. DENTON: If we could skip ahead to Government Exhibit 1202-18.
Q. Again for the the top line here that's highlighted in black that ends in revert to snapshot BK 4-16-2016.
What's the date and time for that entry?
A. The date is April 20, 2016, the time is 17:35 or approximately 5:30 p.m.
Q. Is that local or Zulu time?
A. That would be local time, Eastern Standard Time.

MR. DENTON: Then finally, Ms. Hurst, if we could go to Government Exhibit 1207-30. If we can just blow up the top four or five lines, that would be great.

Q. Sir, what is the date and time the file that was created on March 3, 2016, was last accessed?

A. It was last accessed on April 20, 2016, at 5:43 p.m.

Q. So, I want to pick up from there, sir, if we could.

And Ms. Hurst, can we put up Government Exhibit 1203-38.

Sir, I think this was something we looked at earlier in your testimony yesterday. Do you remember that?

A. Yes.

Q. And you talked about how these were the kinds of files you used to audit user activity on the system?

A. Yes.

Q. So, I want to start with the first line that's highlighted in black there which ends in LS-AL. Do you see that?

A. Yes, I do.

Q. Do you know what that means?

A. That is a directory listing, a listing of all the files and/or directories in this directory on the ESXi server.

Q. And what sorts of files are listed in this directory?

A. These are all the files that make up the Confluence virtual machine. The dot BUDK files are basically virtual hard drives, the VSWP are swap drives, there's the VMX which are

configuration files which describe how the virtual machine is set up as far as processors or memory.

Q. That directory listing, the LS-AL, is that something that happens automatically or is that a user command?

A. That's a user command.

Q. Then, down towards the bottom, we talked a little bit yesterday about the six files that end in dot log. Do you see that?

A. I do.

Q. So if I can ask you, you see the line that ends in VMware-8.log?

A. Yes.

Q. Is there a date and time for that file?

A. Yes, that was created on April 16, around 5:42 p.m.

Q. Did you do anything in the Confluence VM on April 16, 2016?

A. Yes. We changed the administrative permissions, SSH keys.

Q. Then the two files below that, VMware-9.log and VMware.log. Is there a date and time for those files?

A. Yes. They're April 20, at 22:38, which is fairly late, which is 10:38 p.m. And the subsequent one is a couple seconds later.

Q. Did you do anything in the Confluence VM on April 20, 2016?

A. I did not.

Q. If we can go down two lines below that, sir. Do you see the line that ends in RMVMware-9.log?

A. Yes.
Q. Do you know what that means?
A. That means remove or delete that log file.
Q. What about the entry below that that ends in RMVMware.log?
A. RM is remove, and that is a deletion of VMware.log.
Q. Did the defendant have any administrative reason to review log files for Confluence on April 20, 2016?
A. No.
Q. Did you delete any log files from Confluence on the evening of April 20, 2016?
A. No.
Q. As a general matter, would you delete log files in your practice as a system engineer?
A. I would never delete log files. The only time I would possibly delete them is if there was a space issue on the server.
Q. Why wouldn't you delete log files?
A. Log files are an audit trail. They also show performance for problems the server may or may not be having at particular times. They are very important for historical purpose as to how servers are running, and troubleshooting future problems that they may have.
Q. What effect did deleting these log files, VMware-9 and VMware, have on your ability to audit user activity on DevLAN?
A. I wouldn't be able to see what happened during that time

period relating to that virtual machine.

MR. DENTON: Ms. Hurst, if we can bring up Government Exhibit 1202-19 which is another log file from the defendant's DevLAN machine.

Q. Do you see the top line that's highlighted in black there, sir?

A. Yes.

Q. What is the date and time for that entry?

A. That is April 20, at 6:51 p.m. Eastern Standard Time.

Q. What does that top line say?

A. "Current state of the virtual machine will be lost unless it has been saved in a snapshot. Revert to snapshot BKUP."

MR. DENTON: Ms. Hurst, would it be possible to also put up Government Exhibit 1203-25?

Q. So, focusing on the left on 1202-19. Do you recognize snapshot BKUP?

A. As far as the evidence goes, yes.

Q. Is that the same snapshot that was taken earlier that day that's shown in Government Exhibit 1203-25?

A. Yes.

MR. DENTON: Ms. Hurst, we can go just to 1202-19.

Q. Sir, did you revert to snapshot BKUP on April 20, 2016, at 6:51 p.m.?

A. I did not.

Q. We have been talking during your testimony about two

different reversions, first to the April 16 backup and now to this one.

Once a system has been reverted to a snapshot, is there ever a reason to go back like this?

A. No.

Q. Why not?

A. If you're in my line of work, if you revert to a snapshot, there's something that happened to the current state of the machine that is either extremely difficult to fix, or is unfixable. If I were to revert to a snapshot, we would stay on that reverted snapshot until the problem would be solved or a better path could be identified for updating or upgrading that server. We would never go forward again after that fact.

Q. If we can look at the last two lines here that are highlighted in black. Do you see in the middle of the last full line that says "finish revert on virtual machine snapshot-57 snapshot-3"?

A. Yes.

Q. What does that indicate?

A. That indicates that snapshot-3, which if you saw in some of the earlier documentation, that's an internal name for VMware, that that revert finished, and on April 20, at 6:51.

Q. When you say it's an internal name, what is the relationship between snapshot-3 and the description BKUP in that top line?

A. Basically, the BKUP is what they call a friendly name. It is what the person that configures that snapshot to be called for remembering what it is. For example, I name all my snapshots usually with a backup and a date, so I know when that snapshot was taken.

Internally to ESXi or VMware, they have internal names as to the number of the latest snapshot, which in this case was internal snapshot number three.

MR. DENTON: So, if we could then go to Government Exhibit 1202-21, another forensic file from the defendant's computer. Thank you, Ms. Hurst.

Q. Sir, do you see the top line that's highlighted in black there?

A. Yes.

Q. What's the date and time for that entry?

A. The date and time is April 20, 2016, at 6:55 p.m.

Q. What does the rest of that line say?

A. "Confirm delete, are you sure you want to delete this snapshot?"

Q. Under what circumstances would you delete a snapshot?

A. The only reason I would personally delete a snapshot is in the event of a successful upgrade to that virtual machine. I would do that after a period of time that the upgrade had been proven to be successful, typically a week or two, and then we would go back and clean up the snapshots.

Q. On April 20, 2016, did you delete any snapshots of Confluence?
A. I did not.
Q. On that date, did the defendant have any administrative reason to delete snapshots in Confluence?
A. He did not.
Q. Do you see the next line below, sort of starting in the middle, where it says "start remove on virtual machine snapshot-57 snapshot-3"?
A. Yes.
Q. Which snapshot is that referring to?
A. That's referring to the snapshot BKUP.
Q. And did that removal or deletion complete?
A. Yes, it did.
Q. When did it complete?
A. On April 20, at 6:55 p.m.
MR. DENTON: Thank you. We can take that down, Ms. Hurst.
Q. I want to leave April 20 and move forward to sort of late spring, early summer of 2016.
A. Okay.
MR. DENTON: If we can bring up Government Exhibit 1079, please. Can we blow up the bottom e-mail.
Q. Sir, who sent this e-mail?
A. Josh Schulte.

Q. Who did it get sent to?
A. This was sent to our branch, ISB.
Q. Did you receive it?
A. I did.
Q. When was it sent?
A. This was sent on Thursday, May 26, at 12:39 p.m.
Q. What is the defendant asking for in this e-mail?
A. The defendant is asking for admin privileges for a project within Stash called Brutal Kangaroo.
Q. Do you know anything about Brutal Kangaroo?
A. No, not really.
Q. At this time, in May, late May of 2016, was there a process in place for developers to request access to projects?
A. There was.
Q. What was that process?
A. The process was the developers were required to request permission to projects and changes to projects through their branch manager or branch chief, and that branch chief was to send the request via e-mail to our group in ISB.
MR. DENTON: If we can go to the top e-mail in this page, Ms. Hurst.
Q. Who sent this e-mail?
A. I did.
Q. Who did you send it to?
A. I sent it to the defendant, Josh Schulte.

Q. Anyone else?
A. I cc'd -- actually it was to my group as well, to let them know I had completed the work.
Q. When you say you completed the work, what did you do?
A. I added Josh as the admin -- as an admin to the project Brutal Kangaroo.
Q. Did you follow the policy that you just described when you did that?
A. I did not.
Q. After you gave the defendant administrative privileges to Brutal Kangaroo, did you do anything else about that?
A. I did. I realized the mistake I had made, and I went and verbally had a conversation with Anthony Leonis.
Q. Other than that conversation, did there come another time when you had any further conversations with Anthony about Brutal Kangaroo?
A. Yes. A period of time after that, we -- Anthony and I sat down and reviewed all the audit data and configurations for the project Brutal Kangaroo.
Q. Just to be clear, do you remember exactly when those conversations took place?
A. I don't remember specifically. It was a week, maybe two. I don't remember, it was quite a while ago.
Q. You said you reviewed something about the audit for the file?

A. Yes.
Q. Did you have an understanding of why you were doing that?
A. Not specifically, no. It was more of a request from Anthony, and we were having some problems with some of the -- with a developer.
Q. Did Anthony ask you to do anything with respect to Brutal Kangaroo around that time?
A. Around that time, some time after that, I was -- we were requested to remove all administrative controls from that project as well as user access, and only put Anthony down as the sole project admin or person who could access it.
Q. Again, do you remember why you were asked to do that?
A. There was problems with Josh with that project. I didn't get into specifics with it. They just said there was a problem and this needed to be handled.
Q. Other than those couple of things you've just now described, did you ever do anything else in connection with Brutal Kangaroo?
A. No.
MR. DENTON: Thanks, Ms. Hurst. We can take that down.
Q. Sir, I want to ask you to focus on the spring of 2017 for a moment, okay?
A. Okay.
Q. Did there come a time in that period when you learned that

information from EDG had been posted on WikiLeaks?
A. Yes.
Q. Were you working that day when you learned that?
A. I was.
Q. What happened?
A. We were notified some time midmorning that a lot of the tools and things that we did were posted to WikiLeaks under a project called Vault 7. There was a lot of confusion as to what to do.

Eventually throughout the course of the day, we ended up shutting down access to the network by disabling all the user accounts and shutting off the internet as well.
Q. When you say "the network," what do you mean?
A. The DevLAN network was -- we turned off all the user accounts so no one could log in.
Q. Why did you do that?
A. That was at the request of our management to try and preserve what was left on the system so that the FBI and folks could come and we could start figuring out what happened.
Q. What effect did disabling all of the user access to DevLAN have on the work of EDG?
A. It shut EDG down. No one could do anything for a long period of time.
Q. Are the servers and various components that made up DevLAN still in your server room at the CCI office?

A. No, everything has been removed and is either in FBI custody or in secure storage.

MR. DENTON: Just have a moment, your Honor?

THE COURT: Yes.

MR. DENTON: Nothing further, your Honor.

THE COURT: Ms. Shroff.

CROSS-EXAMINATION

BY MS. SHROFF:

Q. Good morning, sir.

A. Good morning.

Q. Let me just start with the access logs that Mr. Denton showed you, right?

A. Okay.

Q. And he showed them to you a couple of times, right? He showed you the access log and then he showed you a time next to it. Correct?

A. Yes.

Q. And he focused on it yesterday in direct and again this morning, correct?

A. Yes.

Q. Sitting here today, do you know who accessed those logs?

You don't know, right?

A. I'm sorry, in regards to?

MS. SHROFF: Could you pull up the exhibit for him.

A. We've looked at a lot of logs. I'm not sure which one

you're referring to.
Q. That's all right. They'll pull it up in a minute. Just give it a second. Do you have a copy of the documents in front of you, sir?
A. I do not.
Q. Okay. Let me see if I can help you out. It's Government Exhibit 1207-27 and Government Exhibit 1207-30. Do you want me to show them to you, sir?
A. Yeah, if you don't mind.
Q. Okay.
THE COURT: What are the numbers again, Ms. Shroff?
MS. SHROFF: 1207-27 and 1207-30.
THE COURT: Thank you.
Q. Looking at these logs, you said they're logs, right?
A. These are not logs.
Q. I'm sorry?
A. These are not logs.
Q. Okay.
A. These are directory listings of the Altabackup which was an NFS share on the NetApp used for backup purposes.
Q. Okay. It tells -- whatever they are, it tells you, and you testified on direct that you can read the access times, correct?
A. You can see the access times, yes.
Q. From seeing the access times, can you see if whatever was

accessed was ever downloaded?
A. We can see that it was accessed at a specific time, which usually the --
Q. I'm not asking you what it usually means. I am asking you, if you know, sitting here today, from this document, that it was actually downloaded; yes or no?
A. Yes.
Q. You can tell sitting here today that something was downloaded after an access?
A. Data access usually means a download.
Q. I didn't ask you what it usually means. I'm asking you whether you can tell.
A. Not from this document, no.
Q. Exactly. And you cannot tell from this document -- and by this document I mean 1207-27 or 1207-30 -- sitting here today, sir, you cannot tell whether anything was copied after access. Correct?
A. No.
Q. Okay.
MS. SHROFF: You can take that down.
Q. You talked a lot on direct about the system, correct? This DevLAN system?
A. Yes.
Q. Okay. And you testified, and correct me if I'm wrong, you said that you thought it was a secure system. Is that what you

said?
A. It was fairly secure.
Q. Fairly secure?
A. Hmm-hmm.
Q. You work at the CIA?
A. I do.
Q. I am assuming the CIA is not in the business of running a system that's fairly secure. Correct?
A. It depends on the use and purposes of the system.
Q. Okay. Well, let's talk about the use and purposes of the system.

You testified that -- you just said, actually, fairly secure, right?
A. Yes.
Q. You remember meeting with the FBI about in 2017?
A. Yes.
Q. And you met with them several times, correct?
A. Yes.
Q. And they spent an inordinate amount of time talking to you about this system, correct?
A. Yes.
Q. And one of the things they asked you to do is to describe the system to them, correct?
A. Yes.
Q. And you used the phrase "wild west."

A. Yes.
Q. Tell us, please, what is wild west?
A. Sure. The system is designed for reverse engineering of malware --
Q. No, no.
A. -- and other tools.
Q. I'm sorry.
A. The system is designed for the creation of malware, tools, nation state tools, things to be used for what COG uses them for.
Q. COG what? I'm sorry. Your voice dropped.
A. The COG network or the operators, the other side who EDG develops tools for.

So, there were some -- there was -- there was user auditing in place. The system was a closed network. You had to have a user password and the specific drop and access to the network to get on.

Q. Okay, that doesn't answer my question why you called it the wild west.
A. Because you can bring malware in and reverse engineer it. We designed the network that it was flexible so that developers could create what they needed to create. It did not have the same use policies as some of the other networks the CIA ran because the nature of the work.

Everyone on the DevLAN network, all the developers

were admins over their own box. They could create and do whatever they needed to do on their own workstation. It is that way because they were developers.

Q. You finished? Did you finish your answer, sir?

A. I'm done.

Q. Okay. So you called it the wild west because you thought it was a wild system; is that right?

A. I called it the wild west because, compared to the other systems that we ran, it was pretty open.

Q. Right. So let's talk about this pretty open system that you had. Right?

A. Yes.

Q. People developed malware on it, correct?

A. Correct.

Q. And malware is just a way to infect another system, correct?

A. Yes.

Q. Malware is something that you create when you want to insert a virus into a computer and shut somebody else's computer down, correct?

A. Yes. But not for the nature of what we did. What the developers did for EDG.

Q. Right. They wanted to steal somebody else's data?

A. Yes.

Q. Okay. Regardless of what they wanted to make the tool for,

it was malware, correct?
A. Functionally, yes.
Q. How many developers were there developing malware?
A. I would say probably 120 to 150. I don't know the exact number.
Q. Okay. When you worked on DevLAN, you knew, did you not, that there were shared passwords, correct?
A. Yes.
Q. And you knew that people accessed each other's projects, correct, on DevLAN?
A. Yes, it was a collaborative environment. That's the way typical development shops work.
Q. It's collaborative and open, correct?
A. Open, yes.
Q. Right. And you told the FBI, did you not, that it was wide open, correct?
A. I did.
Q. Right. And you told the FBI that there were no controls on it, correct?
A. I did at the time, yes.
Q. Right. And by "at that time," you mean at the time far closer to when DevLAN was being used at the CIA than now, correct?
A. I don't understand your question.
Q. Okay. Let me try it again. When you met with them, it was

closer to the time of when you discovered WikiLeaks, correct?
A. It was after the leak, yes.
Q. Right. So things were fresher in your mind than they are now, right?
A. They were fresh in my mind.
Q. Good.
A. However, some of the things that they were referring to, things like specifically Altabackup --
Q. Sir, can I stop you here for a minute.
MS. SHROFF: Your Honor, could the witness just be instructed to answer the question.
THE COURT: David, listen to the question, answer the question.
THE WITNESS: Yes, sir.
THE COURT: If there are other things you want to talk about, Mr. Denton will bring that up.
THE WITNESS: Excellent. Sorry.
Q. You told the FBI, did you not, that there was not too much logging turn-on on DevLAN, correct?
A. Yes.
Q. And you told the FBI, did you not, that it was easy for somebody to connect the DevLAN box to the internet, correct?
A. I don't remember saying that.
Q. Do you remember saying to the FBI if someone wanted to connect a DevLAN box to the internet, the person would have

only had to just switch the DevLAN and FIN fiber or ethernet cable in the back of the box. Do you remember saying that?

A. If I said it according to the -- then I must have said it. I don't remember sitting here today.

Q. Let me see if I can refresh your recollection by showing you 3515-13, page five. 3515-13, page five.

MS. SHROFF: May I approach, your Honor?

THE COURT: Yes, you may.

(Pause)

A. I remember that, yes.

Q. Good. And then you went on to tell the FBI that no security monitoring or tool would have prevented someone from doing so, correct?

A. Correct.

Q. And after that, they asked you if you knew of anyone who had done that, and you said no; correct?

A. Correct.

Q. Where did you sit, sir? Did you sit in an office?

A. Yes.

Q. In a closed office?

A. Yes.

Q. Outside of the cubicles?

A. Yes.

Q. Nowhere near the people who were sitting in the cubicles?

A. There were only about six or seven people who sat in our

actual office.
Q. Okay. And your office was locked you said, correct?
A. Yes.
Q. And you said you were sitting in a vault, you said, right?
A. Yes.
Q. You locked in and out of that, you clicked in and clicked out?
A. Correct.
Q. Outside of your office, how many other people had a FIN?
A. How many FIN drops did we have. We had approximately -- 50 to 75.
Q. 50 to 75 FINs, right?
A. Yes, ma'am.
Q. How many DevLANs?
A. Quite a bit more. Probably 200.
Q. So at the least we have 50 FIN cables, and 200 DevLAN cables, right?
A. That would probably be an accurate assessment.
Q. Fair to say you spent a majority of your time doing work in your office, correct?
A. I would say I spent some time in my office. I spent time on the floor, I spent time in the server room.
Q. We'll talk about the server room in a minute. But mainly you were working, correct?
A. Yes.

Q. It wasn't a secret, sir, was it, that you could switch cables?
A. No.
Q. Okay. You testified on direct that if somebody did that, right, according to your testimony to Mr. Denton here, that Websense would immediately notice, right?
A. It would notify on the screen, yes. We would see a work station connect.
Q. Do you remember a time when an employee plugged in a laptop with wi-fi?
A. I do.
Q. It took four hours for somebody to figure out it had been plugged in, right? Four full hours?
A. Yes.
Q. And four full hours before they even knew that a laptop with internet was plugged in, right?
A. Yes.
Q. Websense didn't pick it up, right? Somebody just happened to see it?
A. No.
Q. Right. By the way, could you tell me what fast IOC internet network means?
A. That was FIN, if I were correct. It was -- basically, FIN was a unclassified CIA attributable network that was connected with a 45 meg internet circuit. It's called fast IOC network.

Q. It was a pretty good network?
A. It was okay, yes.
Q. Yeah. Now, you talked about how the security system was set up. Let's just keep talking about that, okay?
A. Okay.
Q. Do you recall at one point telling the FBI that the security logging capability on Stash was set at default. Do you remember that? Just --
A. Initially, it was set to default.
Q. Right. Default is the lowest level of logging capability, right?
A. Yes.
Q. Absolutely the bottom rung, right?
A. Default is default, so whatever -- default means different things for different applications.
Q. Right. And this is Stash, right? You testified Stash is one of your most guarded code repositories, right?
A. Yes.
Q. It's set at default, the logging on it, right?
A. Yes.
Q. You also testified quite a bit, did you not, about this phrase of latency, right? Remember that?
A. Latency between --
Q. I just asked you if you remember testifying about it.
A. Yes.

Q. Now, you testified about latency because you were asked by Mr. Denton about access to DevLAN from Foreign Office East and Foreign Office West, correct?
A. Yes.
Q. And you testified, did you not, that -- or Mr. Denton elicited it, that there were so many problems because the internet was so slow, right?
THE COURT: The internet was what?
Q. So slow.
A. It wasn't an internet. It was an extended private encrypted tunnel between CCI East, the CCI, and Foreign Office East and West. It did not traverse the internet.
Q. It did traverse the internet, it just didn't traverse the internet fast or well according to your direct, right?
A. It was running through CIA infrastructure and other private facilities between here and overseas.
Q. Okay. Did you understand my question to mean simply this --
A. Please repeat it then. I understood you said internet, and this wasn't touching the internet.
Q. Let's try it again. People in Foreign Office West --
A. Hmm-hmm.
Q. Right. Had a way to connect into DevLAN here. Correct?
A. Yes.
Q. Okay. And you just testified that it's through an

encrypted tunnel, correct?
A. Yes.
Q. And the whole point of this tunnel is to make sure that whoever is in Foreign Office West knows and can access United States, correct?
A. Yes.
Q. That's the point, right?
A. Yes.
Q. Right. And you testified that this was so slow that you used the phrase "latency," correct?
A. Yes.
Q. And you also testified that you would have personal knowledge because you're one of the people who worked on latency, correct?
A. I'm sorry, I didn't understand. I can't hear you very well.
Q. Oh. Nobody's ever had that complaint before, so thank you.
A. I have a little bit of hearing loss. I apologize.
Q. So you testified that latency was something that you tried to fix, correct?
A. Tried to adjust, yes.
Q. Is it fair to say, sir, that in your weekly activity reports, you did not note working on latency issues?
A. I don't have any specific knowledge either way on that. It was part of the daily activity. We worked on our projects.

Our weekly reports typically focused around projects we were doing locally with the developers, putting and bringing them services, things of that nature.

Q. So it's fair to say, right, that your written weekly report doesn't talk about your work on latency, but you tried to fix the problem, correct?

A. Yes.

Q. Is it your testimony sitting here today, sir, that the CIA still has trouble letting Foreign Office West access information in the United States?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Does the problem still exist, according to you?

MR. DENTON: Objection.

THE COURT: Sustained.

Q. Did the problem still exist in 2016, according to you?

A. Yes.

Q. It existed in 2016. Did you fix it?

A. No.

Q. So, the CIA was aware of a problem and just didn't fix it since 2016?

A. That's correct.

Q. 2017?

A. Correct.

Q. So, according to you, the CIA has a foreign office that

cannot access information in its local office. That's your testimony today?

A. Yes.

Q. Okay. Staying with the system. Just talking still about the security of DevLAN. Do you recall telling the FBI that DevLAN was a mess? Do you remember saying that to them?

A. Not specifically, no.

Q. Take a look at 3513, you still have it in front of you, page three. Page three of five, all the way at the bottom.

A. Okay. Yes. I remember that now.

Q. Right. And you told them DevLAN was a mess, and there was over 100 to 200 terabytes of crap?

A. Yes.

Q. Okay. And they also asked you if there were restrictions, were there not, on DevLAN users' ability to navigate on to Altabackup, correct?

A. Yes.

Q. And you said Altabackup was wide open. Correct?

A. I remember saying that, yes.

Q. Right. And then you said that the only restriction was for someone to know an IP address, correct?

A. Correct.

Q. You also told the FBI, did you not, that it would be easy for somebody to pull down a read only copy of the backups of DevLAN, correct?

A. Backup of -- in the entire DevLAN? Or --
Q. Let's just start with, let's stay with Altabackup. You told the FBI, did you not, that somebody could pull down a read only copy of Altabackup, right?
A. Yes.
Q. And how many people at the FBI -- I mean at the CIA could pull down the Altabackup as a read only copy?
A. At the time that I made that statement, I was ignorant to how Altabackup was set up.
Q. Sir, did you hear my question?
A. I did.
Q. Okay. I didn't ask you if you were ignorant then or any question about that.

And let me just go back to that answer for a minute. Did you tell the FBI that you were ignorant?
A. No.
Q. Why?
A. I believed at the time I told the FBI that I did not know how Altabackup was set up.
Q. Really? Did you tell the FBI, "I don't know how Altabackup was set up so go ask someone else"?
A. No, I said --
Q. No?
A. I said --
Q. Sir, listen to my questions, please.

You did not tell the FBI, did you, that you didn't know the answer; no, right?

A. No.

Q. Right. You didn't tell them, "I'm ignorant about Altabackup, go ask someone else," correct?

A. Correct.

Q. Right. You answered their questions, correct?

A. Correct.

Q. In fact, they came to you with a long list of written questions, right?

A. Yes.

Q. Right. They gave you written questions, you thought about them, and then you answered them, right?

A. Yes.

Q. I mean, it wasn't like the FBI was rushing you, correct?

A. Correct.

Q. They gave you all the time you needed to answer them, correct?

A. Yes.

Q. They even told you that this was a voluntary interview, you didn't have to be there, correct?

A. Yes.

Q. And then they told you if you wanted, you could have a lawyer there, correct?

A. Yes.

Q. And then they told you take as many breaks as you want, correct?
A. Yes.
Q. They thanked you for helping them, correct?
A. Yes.
Q. It was a friendly interview, right?
A. Yes.
Q. You could have told them, I'm ignorant about Altabackup, right?
A. Yes, I could have.
Q. But you did not, right? You did not, correct?
A. Correct.
Q. Okay. Let's talk about tracking bandwidth activity. You never tracked bandwidth activity, right?
A. No.
Q. That's one way to keep track of what is or is not secure, right?
A. It is one way, yes.
Q. You testified about logs, right?
A. Yes.
Q. And you noted the importance of logs, correct?
A. Yes.
Q. Right. And is it fair to say nobody audited logs on the DevLAN system? Just yes or no.
A. We did audit logs.

Q. Okay. Did you tell the FBI that you did not audit logs?
A. As far as relating to user activity.
Q. No, right?
A. No.
Q. Okay. Did you tell the FBI, by the way, that the process for removing people from projects was the same process as adding them on to a project?
A. I don't remember specifically saying that. But ...
Q. Okay. Let's talk about SSH keys, okay?
A. Okay.
Q. Now, you said that 99 percent of the work, and you correct me if I'm wrong, okay, of the work could be done through web interface, and you did not need to go through SSH keys for most tasks.
A. Which applications are we talking specifically?
Q. Any application. For almost any application this would be true, right? 99 percent of the work can be done through a web interface, right?
A. I'm going to disagree with that.
Q. Okay. Tell me which applications would you be able to do 99 percent of the work with web interface?
A. With Atlassian, you can do a lot of the administration of the applications through the web interface.
Q. Okay. Let's stay with that. Okay. Let's break that down. Could you explain to the jury exactly what you mean.

A. A lot of the admin control, how projects were set up, which users had access to which projects, adding people to the wiki Confluence and other things could be done via the web GUI. Web browser.

Q. What is a web interface, by the way?

A. It was whichever browser you wanted to use which was in somebody's work station. It could be -- excuse me. It could be Chrome, it could be Firefox, it could be Internet Explorer.

Q. So the same web browser I have on my iPhone, right?

A. Yeah.

Q. Google, Safari, Yahoo; whatever I want?

A. Fundamentally, it has to be a web browser.

Q. You could log in just like you log into The New York Times, right? You put in thenewyorktimes.com, gives you a prompt, you put in your password, you move right along, correct?

A. Correct.

Q. By the way, once you log in that way, if you don't log out, you remain logged in, correct?

A. Correct.

Q. You could remain logged in for days, correct?

A. I don't specifically recall --

Q. I am just asking you if one could remain logged in for days.

A. I'm not sure.

Q. Okay. You are not sure if a person can remain logged in

for days. Is that your testimony?
A. Yes.
Q. Okay. Let's talk about the Stash backup that was in your home directory. Okay?
A. Okay.
Q. You testified on direct yesterday, I think it was yesterday, that you kept two copies, at least two copies of Stash, correct?
A. Yes.
Q. And you testified that you kept one copy on your home directory, right?
A. Yes.
Q. And then you kept one copy, you put it on a hard drive?
A. Yes.
Q. By the way, before you did that, did you talk to Mr. Leonis about how you were going to back up Stash?
A. No, I worked with Jeremy on what we were going to do.
Q. I didn't ask you about Jeremy.
A. I didn't work with Mr. Leonis.
Q. You did not tell Mr. Leonis that one of the ways you were going to back up Stash was to put it in your home directory. Is that your testimony?
A. Yes.
MS. SHROFF: Can you just pull that exhibit up. 35 -- actually. Hold on for a minute.

Q. When you backed up Stash into your home directory, you made no note of that anywhere, correct?
A. Correct.
Q. Only you knew that you did that, along with Jeremy and Tim?
A. Correct.
Q. Right. And Stash is where your crown jewels are, correct?
A. Yes.
Q. So you took them, and you put them in your home directory, right?
A. Yes.
Q. How many home directories are there at the CIA?
A. That's not an accurate question. If we're talking home directories, it would be on DevLAN.
Q. Okay. Well DevLAN is at the CIA, so I'm sorry. Let me try it again.

How many home directories are there on DevLAN?

A. There was probably over 200.
Q. Right. And each employee has a home directory, correct?
A. Who had an account on DevLAN, yes.
Q. Okay. And so, if one person wanted to send a file to another person on DevLAN, they could literally put the file into the other person's home directory and say to Dave, from Anthony. Correct?
A. I believe that's how some of the developers were set up.
Q. Right. In fact, most developers were set up that way,

right?
A. Yes.
Q. Okay. So, a developer could go into another developer's home directory, right?
A. Yes.
Q. Okay. And you testified on direct that that couldn't be done with your home directory, right?
A. Correct.
Q. And you told the FBI when you met with them that you put one copy in your home directory, correct?
A. Yes.
Q. By the way, when you told the FBI that, you also told them that you put a copy on the hard drive, correct?
A. Yes.
Q. And then on direct you told us that you put this hard drive in a safe in your office, correct?
A. Yes.
Q. And then at some point, when you got rid of the safe, you put it in your desk?
A. Yes.
Q. This is Stash.
A. Yes.
Q. On a hard drive?
A. Yes.
Q. Do you remember by any chance never telling the FBI that

you put this hard drive in a safe?
A. I might have.
Q. Let's try. 3515-09. Here you go, sir.
(Pause)
Q. This is your interview with them in May of 2017, right?
A. Yes.
Q. You tell them that you made a backup, correct?
A. Yes.
Q. Made a backup on April 16, correct?
A. Yes.
Q. You placed the copy on your home drive, on your home directory, correct?
A. Yes.
Q. You never tell them that your home directory is locked at all, correct? But we'll get to that in a minute. Right?
A. Yes.
Q. And then you tell them that you made a separate copy and put it on a hard drive, right?
A. Yes.
Q. And then you told them, they asked you, hey, where's that hard drive, right?
You have to answer verbally.
A. Yes.
Q. The FBI asked you where's the hard drive, right?
A. Yes.

Q. And you said you were not sure if you still had the hard drive, correct?
A. Correct.
Q. Or that if you had wiped the hard drive, correct?
A. Correct.
Q. You never mentioned a safe, correct?
A. Correct.
Q. You never mentioned any vault, correct?
A. Well, it was located inside of a vault.
Q. I am not asking where it was located. I'm simply asking if you told the FBI about that.
A. Yes, no.
Q. You never told the FBI, did you, that you ever moved it to a locked compartment in your desk, correct?
A. Correct.
Q. And you also said that you actually couldn't even recall if you had wiped the information about Stash off of that hard drive, correct?
A. Correct.
Q. And sitting here today, you have not a clue as to where that hard drive is, correct?
A. No, I don't.
Q. You also told the FBI, did you not, in May of 2017, that home directory information was available to everyone with an Atlassian account, correct?

A. The home directory --
Q. I just asked you if you told the FBI that. That's all I'm asking, sir.
A. Yes, I'm sorry.
Q. You did, right?
A. Yes.
Q. You told them that?
Did you tell them your home directory was locked?
A. I don't recall.
Q. And then you told them, again, that it was the wild west, correct?
A. Yes.
Q. You also told them during that same interview, did you not, sir, that anyone could have copied and downloaded the data on Confluence by using vSphere, correct?
A. Yes.
Q. And then you told them that another way to download and copy this data was by cloning, correct?
A. Yes.
Q. And then you told them or it could be done by FSN -- I don't know what this is. FSYNC, correct?
A. I believe the acronym was Rsync.
Q. So that's three other ways using the vSphere, cloning, and Rsync, correct?
A. Yes.

Q. Then you told them that the easiest way to copy this data would be by using vSphere within VMware, correct?
A. Yes.
Q. Enable someone to copy the data quickly, right?
A. Yes. The copy would take some time, but yes.
Q. Then you said you could just walk it out the door?
A. Yes.
Q. Just simply walk it out of the CIA?
A. Yes.
Q. And that's because CIA had no controls, correct?
A. Correct.
Q. Right. You could walk out of the CIA with literally a computer in your hand, right?
A. Yes.
Q. I'm sure Mr. Denton will on redirect ask you if you saw somebody walk out with a computer in your hand. I am assuming you did not, right?
A. No.
Q. But one could.
A. Potentially.
Q. Right. By the way, let me ask you something. You testified about your daily hours at the CIA.
A. Yes.
Q. Right. What time do you generally start work?
A. Usually start at 8:3:0, 9 o'clock in the morning, finished

around 4:30 to 5 in the evening.
Q. Did CIA have flex time, by the way?
THE COURT: What?
MS. SHROFF: Flex time.
THE COURT: Thank you.
A. I'm a contractor. That option is not available to me. I can assume there may be some with the staff.
Q. Did you know of people who started later than you and ended their day later than you?
A. I didn't pay too much attention to what the developers did. I didn't work with them. I worked in a separate office. So I didn't see the comings and goings typically.
Q. I was just wondering if you knew of the CIA policy that allowed for people to start later and end later.
A. Yes.
Q. Okay. Let me stay on April 16. That's the day you testified that you came in on a Saturday, correct?
A. Yes.
Q. And you came in with Mr. Weber, correct?
A. Yes.
Q. And then the other person that was there was Tim, correct?
A. Yes.
Q. And is it fair to say that on that date, you deleted all the secure shell keys, correct?
A. We deleted the keys that would allow me to log into the

servers.
Q. And you testified that at that time, someone named Patrick had an SSH key on Confluence; is that correct?
A. I don't remember that.
Q. You don't remember that?
A. I apologize, I don't. That was a long time ago.
Q. That's all right. By the time you went in on April 16, Patrick had already left the CIA's local office, correct? He had moved on?
A. I apologize. Referring to which Patrick? Schaeffer. Yes.
Q. Okay. And --
A. So if I may correct myself, I had a different Patrick in my head. Could you repeat the previous question for me as to who had the SSH keys.
If it was Patrick Schaeffer, prior to April 16, he may have had a copy of that key to log into the server.
Q. He did, right?
A. Prior to the 16th, yes.
Q. And prior to the 16th, or even after actually on the 16th, Patrick's keys were still there, correct?
A. Before or after? I apologize. After the 16th?
Q. No, no. Before?
A. Before, yes.
Q. But they were left there long after he had left?
A. Yes.

Q. For the foreign office, correct?
A. Correct.
Q. How long had his keys just been there since he left for the foreign office; do you know?
A. The keys were actually, it was one key. And it was shared between --
Q. I appreciate that. My question was far simpler.
A. Okay.
Q. His keys were still there, correct?
A. The key was still there, yes.
Q. Right. He was gone. Correct?
A. Yes.
Q. No need for his key to still be there, correct? He's gone, correct?
A. Incorrect. That was the key that logged on to each of the Linux servers with administrative credentials.
Q. But he is not using the key, correct?
A. Correct, but the key was still used to log into the servers. That was the log-in to the servers. If you delete that key, no one gets into the servers.
Q. You don't have to delete a key after somebody leaves. You simply change a key after someone leaves, correct?
A. You can.
Q. You should, correct?
A. Correct.

Q. You should delete that key after he left, correct?
A. Correct.
Q. That would make for security, correct?
A. Correct.
Q. You did not change that key after he left, correct?
A. Correct.
Q. Okay. Let's see if we can pull up -- let me just ask you this question without an exhibit.

Do you know somebody named Rufus, by the way?

A. Yes.
Q. Rufus had a key, right?
A. I assume that Rufus did. I didn't have too many interactions with Rufus. He did not sit in our office.
Q. Okay. Rufus had a public key on Confluence as of April 16, 2016, correct?
A. I'm going to have to take you at your word on that.
Q. Will you take me at my word that he was no longer in EDG at that time?

MR. DENTON: Objection.

Q. I'll ask it -- did you know if he was in EDG at that time?
A. I don't remember when Rufus left.
Q. Do you know that Rufus' keys after he left were still there?
A. Yes, that makes sense for how SSH keys work.
Q. That's how SSH keys work. You leave EDG, and you leave

your public keys behind. That's how it works?
A. Yes.
Q. Okay.
A. That's how they did it. I was not administrating the service at that time.
Q. That wasn't my question at all, sir.
A. I apologize.
Q. My question for you is, is it good security practice to leave your key after you have left that group or that division or that branch.

Is it not poor security practice to leave your key?
A. Yes it is.
Q. Thank you. In fact, it's basic standard operating procedure, correct, to not leave a key after you've left a group, a division or employment. Correct?
A. Yes.
Q. You testified about other types of public keys on DevLAN, correct?
A. Yes.
Q. And another type of a public key is called a root public key, correct?
A. I don't recall ever talking about root public keys.
Q. Okay. Is there such a thing as a root public key?
A. There are public keys and private keys, in talking about the SSL the TLS.

Q. Is there such a thing as a root key?
A. In regards to?
Q. On servers.
A. I believe so, yes.
Q. Right. You just called it root access, correct?
A. Thank you.
Q. If someone had root access on any one of the CIA's servers, could they not also have root access on Confluence?
A. They would have root access to the server. They would be able to see the files and folders and database, but that would not enable them to log into the web and make changes.
Q. I didn't ask you if they could make changes, sir. I simply asked you a far easier question.
A. Okay. Can you repeat the question, please?
Q. Sure. If somebody had root access on a server, that would give them root access to Confluence, correct?
A. Yes.
Q. Let me see if I can pull up Exhibit 1207-7. Do you see, sir, there is a P for root@Jira.IOC.local?
A. Yes.
Q. You see that?
A. I do.
Q. Does that mean that Jira had root access to Confluence?
A. No. My understanding with this key is, this is a key to log into the Jira application to push code up and things to the

Jira application, not to the server.
Q. So your testimony is, and you've already testified about Jira, I'm going to come back to that. You testified that COG didn't like it, correct?
A. That was my understanding.
Q. All right. We'll come back to that one.
Your testimony is that this section does not mean to you that Jira had root access to Confluence. Is that your testimony?
A. Could you repeat that one more time? I was looking at the exhibit.
Q. That's okay. If could you just pull that back up for -- thank you, sir.
You see that?
A. Yes.
Q. Root@Jira.IOC.local?
A. Yes.
Q. And your testimony sitting here today is that you disagree with me when I say this shows that Jira had root access to Confluence. You disagree.
A. Looking at this key, this appears to be a log in to Jira.
Q. Right.
A. I would -- I can't say specifically if this would allow you onto Confluence or not.
Q. Okay. Thank you. Now, when you said that on April 16,

what you essentially did was you, by deleting keys, essentially what you did is, you changed everyone's password. Right? Is that an easier way to understand that?

You can take this down.

A. Is this a yes or no question or can I explain what we did?

Q. Well, if you want to explain it, but, you know. We all have limited technology.

A. What we did on, when we changed the root key to get in, this was the only key that was used to log in to the operating system of each Linux machine. When we changed that, we changed it for everybody.

Q. Right. But, basically, when you changed that, is that essentially like, everybody comes in the next day, and their keys are no longer working, right?

A. If they tried to log on to the server, they would not be able to get in.

Q. I was trying to make it simple, which would be like if your password was changed and you couldn't log in anymore, right?

A. Correct.

Q. That's all I meant.

You stored the new keys somewhere, right, and you told Tim where you stored them, correct?

A. Yes.

Q. And you stored them in a shared directory, right?

A. Yes.

Q. You gave that directory a name?
A. I don't remember specifically the name of that directory.
Q. You don't remember the name of the directory in which you stored the passwords?
A. I remember where we put it.
Q. Right. Did you give it an Atlassian name, by any chance? Do you remember?
A. I may have, yes.
Q. Right. So you made new keys, then you saved the new keys with the name Atlassian in it. Right?
A. Yes.
Q. Okay. It's not a good way to store a changed password, correct, by using Atlassian in it?
You know what. I'll withdraw that. It's okay.
When you took a snapshot of Confluence VM, right?
A. Yes.
Q. You saved that snapshot, right?
A. Yes.
Q. And then you saved the snapshot as backup before network change, correct?
A. The Confluence, a backup was called backup 4-16-2016.
Q. Okay. When you saved it in your home directory, you never saved Confluence in your home directory, correct?
A. I saved Stash in my home directory.
Q. When you saved it, you don't remember saving it as backup

before network change.

Take a look at 3515-09.

A. So I do remember what you're referring to.

Q. Okay.

A. That backup was not on 4/16. That happened the week following when we moved the Confluence and Bamboo virtual server off of the OSB ESXi server over to ISB ESXi servers.

Q. So you named another move that you made. You named that one backup before network change?

A. Yes.

Q. And is it fair to say that after you made that particular move, you changed the IP information for that VM?

A. Yes.

Q. And when you did that, am I correct that you had to first shut down the VM, right? You shut down that virtual machine, right?

A. Yes.

Q. And then you copied it over, correct?

A. Yes.

Q. And then you copied it over to something called OSB_test_repo, correct? Do you remember that?

A. I do.

Q. Okay. Help me out here. Isn't OSB_test_repo also wide open?

A. I don't remember the specific permissions on that, no.

But --

Q. You told the FBI it was open, correct?

A. I said there were -- I didn't say specifically everything was wide open.

Q. But this one was open, right?

A. I don't -- by the nature of the work that we were doing, that was closed off.

Q. So it was not open is your testimony?

A. That is my testimony.

Q. It's your testimony today that it wasn't open; it was closed off?

A. I believe it was closed up, yes.

Q. And you recall telling the FBI that it was open or you recall telling the FBI that it was closed off?

A. I don't remember specifically referencing that to the FBI.

Q. Okay. All right. Let's talk about this. OSB_test_repo, is that local storage?

A. That's network storage.

Q. It's local, right?

A. Network storage.

Q. Okay. It's storage on the OSB ESXi server, right?

A. No.

Q. It's not?

A. No, it was storage on the NetApp server.

Q. It's storage on the NetApp server?

A. Yes.
Q. You're saying that when you made this move, you moved that VM from that server to its final destination, which is DS000; is that correct?
A. I'm trying to explain.
Q. I don't want you to explain it. Thanks.
A. Yes.
Q. That's where you moved it, right?
A. Yes.
Q. What is DS000?
A. It's referencing the NetApp.
Q. The NetApp?
A. Yes.
Q. Is it your testimony sitting here today that NetApp is open or not?
A. Pieces of NetApp were open.
Q. No controls, correct?
A. Limited control.
Q. By limited control, you mean control that did not even meet standard operating protocol, correct?
A. Yes.
Q. Okay. And by the way, when I say "standard operating protocol," I mean like basic -- like my office would have, right, like we're lawyers' offices, basic protocol, right. Standard --

A. I apologize, I can't answer that. I don't know what, I've been in my environment for quite some time. I don't know what your office's protocol is.
Q. Very fair. But let me ask you this. When somebody issues a standard operating protocol, that is like the very basic level, correct? That is what you must comply with, correct?
A. Okay.
Q. Okay. No, no. Not "okay."
A. Yes.
Q. Yes or no?
A. Yes.
Q. That was confusing, you saying "yes," me saying "okay."
Let's talk about these missing Stash logs, okay? You said that you never would have in a security system or in a secure system lose logs, correct?
A. Correct.
Q. And you were asked about missing logs, correct, missing logs from January 14 to April 21, correct? You remember that?
A. I'm sorry, I apologize, not really. But if it's in the report, I may have talked about it.
Q. Let's look at 3515-09. Page four. You were asked about missing logs from January 14 to April 21, 2016. Correct?
A. Is this -- which exhibit is this? I apologize. I don't have the right -- do I have the right one?
Q. 3515-09.

THE COURT: Here is a copy.

THE WITNESS: Oh. Okay.

Q. You see that paragraph?

A. I'm sorry. Where is it on the page? Page five of 10?

THE COURT: Page four.

Q. It's highlighted for you.

A. It's on the backside. Okay. Yes, ma'am.

Q. Okay. And they asked you about these missing logs, and you said it could be an issue with the server space, correct?

A. Yes.

Q. You said you could have deleted older logs to free up space, correct?

A. Yes.

Q. It's possible, you said, that logs are only kept for 30 days anyway, correct?

A. Yes.

Q. At the same time that they were talking to you about these logs, they also asked you about Stash and how the identifier for Stash could change, correct?

A. The identifier.

Q. Right.

A. Can you tell me specifically where that's referenced?

Q. Sure. Just the highlighted section below. Where you were. Still page four.

A. Still page four.

Q. Right.
A. Oh, yes.
Q. You said you were not sure why they would change, but you thought that IDs could change every time that the Stash service was restarted, correct?
A. Yes.
Q. Now, you testified about server rooms, correct?
A. Yes.
Q. How many server rooms are there at the local facility?
A. We had -- basically two. Three.
Q. Three?
A. Three.
Q. And they're all at the same facility; is that fair to say?
A. Between two floors, yes. The eighth and ninth floors, yes.
Q. They're between two floors, right?
A. Correct.
Q. You badge in, you go in and you work in the server room, correct?
A. At the time only one server room had badge access.
Q. Only one server room had badge access?
A. Yes.
Q. What was the access to the other server rooms?
A. It was open, which means it was inside of a vault, but the room did not have a separate badge or combination on it.
Q. Okay. So, let's start with the one where you badged in.

A. Okay.
Q. They gave you like an access badge. You stuck it on there and you went in?
A. Yes.
Q. At that time there was no requirement for it to be double badged, correct?
A. Correct.
Q. Now you need a double badge, correct? Or do you not know?
A. Well, when I left that group about a year ago, when I left, there was, yes, there was double badge.
Q. Right. But in 2016, you could single badge in, right?
A. Yes.
Q. And once you single badged in, somebody badged in right behind you, correct?
A. Yes.
Q. And there were times, is it fair to say, that you badged in, and another employee is behind you, does not badge in, but walks on in with you, correct?
A. Yes.
Q. Is that called tailgating into the server room?
A. It wasn't a policy at the time.
Q. I know it's never the policy. I am asking you if it happened.
A. Yes.
Q. And it's called tailgating into the server room, correct?

A. Yes.
Q. You testified that there are no desks in the server room; is that right?
A. Yes.
Q. Isn't it fair to say, sir, that even though there are no desks, there are like these standing shelves where people can stand and work?
A. Yes.
Q. Right. So it's kind of like having a desk, but it's like a makeshift desk, right?
A. Yes.
Q. The thing, like, protrudes out?
A. Yes.
Q. You stand there, you do your work?
A. Yes.
Q. And then you leave, correct?
A. Correct.
Q. How many times would you say when you worked in the CIA server room that you saw Post-its with IP addresses in the server room?
A. Frequently.
Q. Say it again?
A. Frequently.
Q. A lot of Post-its with a lot of IP addresses on there, right?

A. Yes.
Q. People left notes for each other in the server room, correct, on Post-its?
A. Yes, generalized descriptions of what things were.
Q. You don't know if they were generalized or not, correct? You would only know if you knew what they were talking about, correct?
A. Correct.
Q. You didn't know what a developer is talking about to another developer, correct?
A. Correct.
Q. And you don't know what a coder is telling another coder, correct?
A. I'm sorry, I didn't understand.
Q. You do not know what one coder is telling another coder, correct?
A. I mean, if it's usually simple little things, server names, IP addresses.
Q. You don't know, right? You're just guessing?
A. I read through a lot of them. I saw what they were.
Q. Okay. So you go into a server room, there are Post-its that people have written to each other, and you read them. Correct?
A. Yes.
Q. So that means everybody else going in and out of the server

room is reading what each developer or coder is saying to the other person.

A. Yes.

Q. Okay. And they're leaving IP addresses for each other, correct?

A. Yes.

Q. And they're leaving IP addresses for themselves, correct?

A. Yes.

Q. Let's go back to talking about your internet computer at the CIA. The FIN. Right?

A. Okay.

Q. And you said that that is the -- is that an unclassified network, the FIN?

A. Yes.

Q. Is it fair to say that one person could connect to another person's FIN?

A. No.

Q. It's not fair to say?

A. No.

Q. There is no way for you, for example, to RDP into another person's FIN?

A. As an administrator on FIN, I had permission to remote desktop into the unclassified FIN network.

Q. Right.

A. Into the machines.

Q. So you could RDP into anybody else's FIN, right?
A. Yes.
Q. What is RDP?
A. Remote desktop protocol.
Q. That just means that you can remote log in to the internet computer of another person there, correct?
A. Yes.
Q. And you would RDP in, not just to fix something, but if you were too tired or too bothered to walk to that particular person's desktop, correct?
A. Occasionally RDP had its ability to fix problems remotely. Yes.
Q. You did that, right, to Mr. Schulte?
A. I have done that, yes.
Q. Many, many times, correct?
A. I don't know about that.
Q. Okay. Well, you did do that, correct?
A. Possibly, yes. It was a long time ago, I don't remember specifically.
Q. I understand.
A. But yes, I logged into multiple users' FIN machines if they were having connections problems to the internet or other issues.
Q. Okay. When you did that to Mr. Schulte, did he seem to care?

A. Not that I can recall.
Q. Let's see if we can talk about the Altabackups, okay?
A. Okay.
Q. Is it a fair statement to say that there were no restrictions on who could access Altabackup?
A. It's not a fair statement.
Q. It's not a fair statement?
A. No.
Q. In your opinion, what were the restrictions on Altabackup?
MR. DENTON: Objection.
THE COURT: The objection is?
MR. DENTON: He's not an expert. Your Honor, she's asking for his opinion.
THE COURT: Overruled.
A. Repeat the question please?
(The record was read)
A. In my opinion, I did not know what the restrictions were. And I assume they were wide open.
Q. Let's see if we can pull up Government Exhibit 1202-8. Could you just highlight there or I'm sure it's obvious. But you see where it says -- and I think you testified about this. It says VMS.NFSmount.error.perm.denied, and then that signal and then key. Correct?
A. Yes.
Q. And you said on your direct that that was an attempt by

Mr. Schulte to mount Altabackup to his work station at the CIA. Correct?

A. Yes.

Q. Now, you've testified here and you also told the FBI, did you not, that if somebody knew an IP address, they would simply be able to access Altabackup. And, in fact, you just testified that Altabackup was wide open, correct?

A. Yes.

Q. Sitting here today, sir, do you know what IP addresses had permission to mount Altabackup?

A. I do not.

Q. Do you know sitting here today, sir, how many IP addresses allowed for the mounting of Altabackup?

A. I do not.

Q. Is it fair to say, sir, that any virtual machine on the ESXi server could mount Altabackup, literally any VM?

A. I can't answer that question. I don't know.

Q. Sitting here today, sir, do you know what a test VM is?

A. Yes.

Q. What is a test VM, sir?

A. Test VM is a virtual machine. It could be any operating system that's used for -- in the purpose of EDG development of code. It's set up, it runs, you do what you need to test what you need to test, and you shut it down.

Q. And when you say you test what you need to test, or you run

what you need to run, you're generally testing malware, correct?
A. Yes.
Q. And you're generally testing a virus, correct?
A. Yes.
Q. And anyone in EDG who ran a test VM could mount Altabackup, correct?
A. I can't answer that.
MS. SHROFF: You can take that one down, please.
Q. Now, you testified and I think you told the FBI this as well, that in your opinion, Mr. Schulte knew the IP addresses for the NFS Altabackup mount, correct?
A. Yes.
Q. Could you tell the jury what NFS is, just remind them.
A. Network file system. It is a location on the network that is more or less specifically Linux computers can connect to, to write their files up to say backups. It is a network resource for saving files, but for Linux.
Q. Just a file share, right?
A. Basically.
Q. You share files on Window, you share files on Linux, correct?
A. Yes.
Q. You like Windows, correct?
A. Yes.

Q. You don't like Linux, correct?
A. Correct.
Q. And sitting here today, sir, do you know how many other people knew the IP address for the NFS Altabackup?
A. I don't know.
Q. You have no idea, right?
A. No.
Q. In fact, nobody even kept track of that at the CIA, correct? Certainly not you, right?
A. Not me.
Q. And I am correct that you did tell these FBI agents and you spoke to all three, right? You spoke to Special Agent Donaldson, right?
A. I spoke to a lot of FBI agents.
Q. Special Agent Schlesinger, correct?
A. Okay, yes.
Q. Evanchec, correct? A lot of them?
A. I don't remember the names.
Q. Fair enough. And you told these FBI agents, did you not, that in your opinion, Altabackup was wide open. That's the phrase you used, right?
A. Yes.
Q. You told them, did you not, that it was up to each user to connect their own network drives to their work stations, correct?

A. Yes.
Q. Any user could do that, correct?
A. Yes.
Q. And you also told the FBI, did you not, when you spoke to them, that there was a CIFS access to Altabackup, right? Yes?
A. I don't remember that. I don't recall that. I apologize.
Q. No, no, it's okay. It's been a long time. Take a look at 3515-13.

MS. SHROFF: Your Honor, would this be a good place to stop for the 11 o'clock break?

THE COURT: Yes, we'll take our morning recess. We'll resume at quarter after.

(Recess)

(In open court; jury present)

THE COURT: All right, Ms. Shroff.

MS. SHROFF: Thank you, your Honor.

BY MS. SHROFF:
Q. Sir, right before we broke, we were talking about CIFS access to Altabackup. Do you remember that?
A. I do remember it.
Q. You told the FBI that there was CIFS access to Altabackup, correct?
A. I don't recall saying that.
Q. Can you just take a look, I think it's before you, 3513, page two. Do you have it there still?

A. Was that 13 you said?
Q. Yes, sir. Page two of five.
A. Okay. At the bottom that's highlighted?
Q. Yes, sir.
A. Yes, I --
Q. It's fair to say that you also told them, did you not, that any Windows user could mount Altabackup that way, even if the auto mount was not enabled. Correct?
A. If I can review, one second.
I see that.
Q. Okay. And is it fair to say, sir, that you deleted the CIFS share from Altabackup on March 1st; is that correct?
A. That may be correct, yes.
Q. Do you remember what year of March 1st you deleted that?
A. It was a while ago. 2016, I don't remember.
(Continued on next page)

BY MS. SHROFF:

Q. Well, it's not 2016.

A. I'm sorry. Two thousand -- I'm sorry. I got my years messed up a little bit. 2017.

Q. Right. March 1 of 2017, correct?

A. Yes.

Q. And until March 1 of 2017, the CIFS share for Altabackup was still up, correct?

A. Yes.

MS. SHROFF: Now, let me see if I can show you what is 1203-28.

Q. Now, on here, do you see -- it is the next command, that connects the Altabackup to the Doxygen server?

A. Can you show me specifically?

MS. SHROFF: Are you sure that's the right document?

A. OK.

OK.

MS. SHROFF: You can take that down for a minute.

Q. Am I correct, sir, that the Doxygen server is another VM that runs on the ESXi server?

A. I will have to take your word for it. I have no knowledge of that server.

Q. OK. Do you know anything about the Doxygen server?

A. I do not.

Q. Do you know whether or not it has wide access; it's called

a wide-access server?
A. I know nothing about that server.
Q. Do you know whether the CIA has a Doxygen server?
A. I do not know what that server is or what its purpose is.
MS. SHROFF: Now, let me ask you, if I may, to pull up 1251.
Actually, I'm sorry. I changed my mind. Could you pull up Government Exhibit 601 for me.
Q. This is a four-page document that you testified to on your direct, correct?
A. Uh, yes.
Q. Did you create this document, sir?
A. Uh, I don't believe that I created this one. I believe Tim may have created this.
Q. OK. Did you review it with the government before your testimony here?
A. I do not recall reviewing this with the -- with --
Q. Did you review it with Tim?
A. Probably back in the day, yes.
Q. OK. All right. So let's see if we can talk about the firewalls that you testified to. OK?
A. OK.
Q. Could you point out for the jury where you see the firewalls on this document?
A. This document is a copy of DevLAN. There were no firewalls

on DevLAN except on the Hickok network.
Q. Right. So let's just point the firewalls out, and I think that's on page 3, right? Is that correct?
A. Let me see.
OK.
Q. Am I correct that the thingamajiggies that have, like, a play sign, those are the firewalls?
A. Probably, yes.
Q. OK. Just so that the jury knows, it's the one that --
MS. SHROFF: I can't. I don't know how to do this.
Q. But this and this is the firewall, right, according to your diagram?
MR. DENTON: Objection.
THE COURT: Overruled.
Q. Is that right? Are those the firewalls?
A. Looking at the -- yes. I'm looking --
Q. OK.
A. I'm looking at the firewalls, looking at your descriptions, yes.
Q. OK. Thank you, sir.
MS. SHROFF: Let's go to page 4.
Q. On page 4 -- you testified about this, right? Page 4 says that the only traffic that goes into and from DevLAN, right? You see that it goes into and from, right?
A. OK.

Q. Do you see that on the top?
A. Hickok is --
Q. Yeah. So it says the only traffic allowed into and from Hickok, right?
A. Yes.
Q. DevLAN and COG, includes SSH, correct?
A. Yes.
Q. So if someone hacked into Jira --
A. Yes.
Q. -- they could SSH into DevLAN.
MS. SHROFF: Could you go back and show him.
Q. Am I correct?
A. I'm not 100 percent certain on that. I don't remember all the firewall rule sets, but --
Q. The firewalls are right there. Take a look.
A. There's rules set within the firewalls that allow for traffic to be stateful and non-stateful, so if the -- there were a lot of firewall settings on that firewall. I don't remember them personally.
Q. Well, take a look here at the firewalls.
A. Uh-huh.
Q. The Palo Alto firewall, is this something you buy -- I can go buy that, right?
A. Yes.
Q. Right. And anybody can go buy that, right?

A. Yes.
Q. How about this ASA firewall, also anybody can go buy it?
A. Right.
Q. Right. So your testimony is that if someone hacked into Jira, they could just SSH into DevLAN, you can't answer that question because you don't know the type of the firewall?
A. I know the type of the firewall.
Q. OK.
A. I do not know what the rule sets were within that firewall.
Q. Right. So you just don't know; they could or they could not, correct?
A. They could or they could not.
Q. Right.
A. That is an accurate statement.
Q. Right. It is equally plausible that you could, correct?
A. Yes.
Q. Equally plausible that you could not?
A. Yes.
MS. SHROFF: Let's just go to page 2 of 2 or 2 of 4.
Q. Can you, looking at that chart, tell me, sir -- I don't know how to take off the purple, so ignore it. OK?
A. OK.
Q. So you see Jira down there?
A. Yes.
Q. This diagram does not tell you --

THE WITNESS: Oh, I'm sorry. Oh, there. Gotcha.

MS. SHROFF: Thank you, sir.

Q. This does not tell you, does it, how Jira was backed up?

A. Jira was not backed up.

Q. OK. Your testimony is Jira was not backed up?

A. If I may correct? I believe Jira was backed up. I don't remember specifically everything that was in Altabackup.

MS. SHROFF: All right. Let's just put this one aside and go to 1207-36. OK?

Q. Now, there is a folder for Jira on Altabackup, right?

A. Yes.

Q. And this shows that the Jira folder was modified on April 13, 2016, correct?

A. Yes.

Q. And it also shows that Jira is backed up to the Altabackup, correct?

A. Yes.

Q. So it's not just --

MS. SHROFF: Going back to 601, page, I think it was 2. 3, maybe?

Q. So it's not just the HTTPS or the SLDAP or the SMTP and SSH allowed by the firewall, correct?

A. Uh --

Q. Take a look --

A. I don't -- I don't know how that backup was being

performed, but you can use the SSH protocol to run a secure copy through it --

Q. Right.

A. -- which would be allowed through the firewall.

Q. Right. So you agree with me now, do you, that the firewall allowed for an NFS connection from Jira to Altabackup. Right?

A. Yes.

Q. All right. So then anyone on Jira could have copied any file from Altabackup?

A. Anyone who had access to Jira.

Q. Exactly.

A. Yes.

Q. Anyone who had access to Jira could copy any file from Altabackup, right?

A. Yes.

Q. All righty then.

Now, sitting here today, you have no idea if there were any other connections that these firewalls allowed, correct?

A. Correct.

Q. And sitting here today, you have no idea what the settings on this firewall were in 2016, correct?

A. I do not remember that, no.

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

Could I just have one moment, your Honor?

THE COURT: Yes.

MS. SHROFF: Now let me just for a minute go back, if I may, to 1207-7.

Q. Now, if I could go back, and I think I asked you about this again, but just bear with me. OK? Let's just go back to the Jira root thing. Right there.

A. OK.

Q. Now, you testified that this is the authorized key file on Confluence that you edited on April 16, 2016, correct?

A. I can't specifically memorize the keys. This is obviously to connect to the Jira server.

Q. Right.

A. I don't know if this would work on the Confluence server.

Q. No, I didn't ask you that. Remember you testified that you went in on a Saturday and you changed all the keys?

A. Right. I don't -- remember, we generated new keys, and these were the authorization keys to log in to the OSB server.

Q. But these are authorization keys prior to April 16; these were authorized keys, correct?

A. Yes.

Q. So Jira here was an authorized key prior to April 16, right?

A. Yes.

Q. So Jira had access to Confluence because it's an authorized key, correct?

A. Yes.

Q. And if you had root on Jira, you had root on Confluence, correct?

A. Yes.

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

Q. Now, could you just tell me, sir, in your opinion, what is a hackathon? Do you know what a hackathon is?

A. I do.

Q. Did the CIA run hackathons?

A. Yes.

Q. And when they ran hackathons, did they have a whole group of people sort of having like a fun day doing hacking stuff, whatever that is? I don't know.

A. Yes.

Q. And how many people would you say from the CIA participated in this hackathon?

A. I didn't have too much involvement with that. My recollection was anywhere from 12 to 13, 20 people.

Q. And each one of these 20 people were given a special laptop, correct, to participate in this hackathon?

A. Yes.

Q. And these laptops, each one of them for all of these people that were doing this hackathon, all of these laptops were connected to DevLAN, correct?

A. Yes.

Q. And each one of these laptops had full access to DevLAN,

correct? Yes? Full access to all of DevLAN --
A. They received IP addresses on the network. I -- looking back, I believe we did set up -- some people already had access to the network. Already they were DevLAN users, and I believe there were some folks that may have come in that accounts were created.
Q. Right. So people had access already, new people came in, they were also given access to DevLAN so everybody could participate in this hackathon?
A. Yes.
MS. SHROFF: All righty then.
I have nothing further. Thank you.
THE COURT: Mr. Denton.
MR. DENTON: Thank you, your Honor.
REDIRECT EXAMINATION
BY MR. DENTON:
Q. Sir, do you remember just now Ms. Shroff was asking you a series of questions about Jira?
A. Yes.
Q. When she was asking you questions, she didn't draw a distinction between the Jira program and the Jira server. Do you remember that?
A. Yes.
Q. Did everyone who had access to the Jira program have access to the Jira server?

A. No.
Q. Where was access to the Altabackups within Jira?
A. They were access -- can you rephrase the question, please?
Q. Was access to the Altabackups through the Jira program or through the Jira server?
A. The Jira server.
Q. Did every Jira user have access to the Altabackups through the Jira server?
A. No.
Q. Did Atlassian administrators have access to the server?
A. Yes.
Q. Now, she asked you a lot of questions just generally about the security practices within the CCI building. Do you remember that?
A. Yes.
Q. When you get to the CCI building, do you have to go through a gate?
A. Yes.
Q. Who's standing at that gate?
A. Armed guards.
Q. What are they armed with?
A. M16s, riot shotguns, things of that nature.
Q. What do you have to do to get by them?
A. Present credentials, a badge.
Q. What do you have to do to get that badge?

A. You have to go through a year or more of background investigation and polygraphs.
Q. Once you get past that gate and those guards, how far does that get you?
A. It gets you to the parking lot.
Q. What do you have to do to get into the building?
A. You have to badge access through a main catcher-type turnstile and provide a valid badge and a PIN.
Q. When you go up to your office, how do you get into your office?
A. I have to present a badge to the badge reader to unlock the door.
Q. Can you go into somebody else's office?
A. If I have access.
Q. What if you don't have access?
A. It will not allow me in.
Q. Was that true for that entire building?
A. Yes.
Q. Was there anyone in that building who did not have to go through that process?
A. No.
Q. Now, Ms. Shroff asked you a lot of questions about the Altabackups, and she asked you at one point who could pull down a copy. Do you remember that?
A. Yes.

MR. DENTON: Ms. Hurst, could we put up Government Exhibit 1202-18.

Q. We've looked a lot at this. After the reversion to snapshot BK 4-16-2016, did the defendant have access to the Altabackups?

A. Yes.

Q. Could he pull down a copy of the Altabackups?

A. Yes.

Q. And do you remember Ms. Shroff asking you some questions about things you said about ways to copy the backup?

A. Yes.

Q. And you talked about vSphere and Rsync, is that right?

A. Yes.

Q. Is vSphere a computer program?

A. VSphere is an application that is used to manage ESXi servers.

Q. Like the OSB ESXi servers?

A. Yes.

Q. When you say used to manage servers, does it manage the virtual servers that are running on that?

A. Yes.

Q. So is vSphere something that you'd use to manage the Confluence virtual server on the OSB ESXi machine?

A. Yes.

Q. Did anyone on DevLAN have access to vSphere?

A. There were multiple copies of vSphere. There was one running for the infrastructure virtual machines that ISB managed, and I believe there was a copy of it running on that server. However, I believe it was not working. We had problems on vSphere. It was a long time ago.

Q. Let me put it this way. Did the fact that you had a DevLAN account mean that you could access vSphere?

A. No.

Q. And Rsync, is that a computer command?

A. It is.

Q. What kind of command is it?

A. It's a Linux command.

Q. And what is it a command to do?

A. Copy.

MR. DENTON: Could we put up Government Exhibit 1207-30, and again just blow up the top few lines.

Q. Now, do you remember when Ms. Shroff was asking you questions about this?

A. Yes.

Q. And she said she wasn't interested in what usually would change the date accessed?

A. Yes.

MS. SHROFF: Objection to the characterization, your Honor.

THE COURT: The jury will determine that.

MS. SHROFF: Thank you.

THE COURT: The objection's overruled.

BY MR. DENTON:

Q. Is Rsync something that would change the date accessed?

A. Yes.

Q. Now, do you remember Ms. Shroff asking you about a Windows version of the mount on the Altabackups?

A. Yes.

Q. Something called CIFS, right?

A. Yes.

Q. Now, you testified on your direct examination about something called Active Directory, right?

A. Yes.

Q. What does Active Directory do?

A. Active Directory is a product from Microsoft running Windows server that allows you to create users in a bunch of computers together, what's called a domain. It's just managing users; their accounts; servers; permissions, primarily; and there's a whole host of other things you can do with it.

Q. And is CIFS linked to Active Directory.

A. Yes.

Q. What does it mean to say that it's linked to Active Directory?

A. CIFS, more properly called, is tied into Active Directory via the NetApp. It actually has a workstation account on the

domain and participates in the domain so that you can define username and passwords that have the ability, are allowed to access files and photos within that CIFS directory.

Q. Does it limit who can access a CIFS directory?

A. It can, yes.

Q. Now, Ms. Shroff asked you about connecting computers to FIN and to the internet.

A. Yes.

Q. Do you remember that?

A. I do.

Q. She asked you about a particular incident where a laptop was connected to the network. Do you remember that?

A. Yes.

Q. After that incident happened, did you have to take any corrective measures?

A. Yes. We basically rebuilt the entire network. We formatted all workstations, all servers, every piece of equipment, and rebuilt everything from scratch.

Q. Why did you do that?

A. It was a direction from our front office. They did not want any -- anything that may have lingered or possibly on the network.

Q. And did that come about because your branch had detected that this had happened?

A. Yes.

Q. Do you remember being asked some questions by Ms. Shroff about whether any virtual machine could connect to the Altabackups?
A. Excuse me.
Yes, I do.
Q. And you said you couldn't answer that question, right?
A. That is correct.
Q. Did you need more information to answer that question?
A. I needed a lot of, more information.
Q. What more information would have helped you answer that question?
A. The primary, primary piece of information I would need would be the IP addresses that were on the virtual machines. Also, it would also need the corresponding what is called an export list on the NFS mount on which IP addresses were allowed to connect. I did not have either of those info -- either of those pieces of information to accurately answer that question.
Q. Do you know for sure that some IP addresses were not able to connect to the Altabackups?
A. Yes.
Q. But off the top of your head, you don't know exactly which ones?
A. I do not. I did not virtually set up that mount point, no.
Q. OK. Finally, I just want to talk about the security of the system in general. You talked a lot about how it was set up to

let people do their work. Do you remember that?
A. Yes.
Q. Did you rely on those people for security on the network?
A. Yes.
Q. How did you rely on them?
A. Everyone was cleared to a top-secret SCI level. There is an expectation of trust that people were going to follow some basic, fundamental rules, and in following those rules, they would be allowed some additional privileges on the network that they would be able to create their work.
Q. And was there any particular trust for the people who were made administrators on the network?
A. Yes.
Q. Why?
A. You have a screen-user access, as they call it. You have the ability to directly manipulate the network. In the boxes, computers and systems that you had direct access to, you could change them for the good or for the bad.
Q. Did the sorts of policies that were in place to provide security with respect to regular users apply to system administrators?
A. No.
Q. Did they apply to the defendant when he was a system administrator?
A. Yes.

MR. DENTON: No further questions, your Honor.

THE COURT: OK. You're excused, David. Thank you.

THE WITNESS: Thank you.

(Witness excused)

THE COURT: Call the next witness.

MR. LAROCHE: Your Honor, the government calls Patrick Leedom.

PATRICK LEEDOM,

called as a witness by the government,

having been duly sworn, testified as follows:

THE COURT: Please sit down, Mr. Leedom.

THE WITNESS: Thank you, your Honor.

THE COURT: Pull yourself right up to the microphone.

All right. Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. LAROCHE:

Q. Good morning, Mr. Leedom.

A. Good morning.

Q. Did you graduate from college?

A. Yes, I did.

Q. From what college?

A. I graduated from the University of Colorado at Colorado Springs.

Q. What's your degree in?

A. I have a bachelor's of science in computer science.
Q. Are you currently employed?
A. Yes, I am.
Q. Where are you employed?
A. I work for the MITRE Corporation.
Q. What is the MITRE Corporation?
A. The MITRE Corporation is a not for-profit company that operates FFRDCs.
Q. What is an FFRDC?
A. An FFRDC stands for federally funded research and development center. It's essentially a government-funded entity that provides research and development to the government.
Q. How long have you been at the MITRE Corporation?
A. About six years or so.
Q. What's your current position?
A. I'm a lead cyber security engineer, and I manage about five employees.
Q. Does that management role have a title?
A. Yes, it does. It's called a group leader.
Q. What do you do at MITRE as a lead cyber security engineer?
A. I'm a contractor to the Federal Bureau of Investigation.
Q. What does it mean to be a contractor to the FBI?
A. For me, I perform the role of a computer scientist for the bureau.

Q. And how long have you been doing that?
A. For most of my time in the company.
Q. Do you work within any particular unit at the FBI?
A. Yes, I do. I support A unit called the technical analysis unit.
Q. And is unit that within a particular FBI division?
A. Yes, it's in the cyber division.
Q. What is the cyber division of the FBI?
A. FBI's cyber division investigates cyber cases or computer-related cases.
Q. And you said that you're in the technical analysis unit within that division, is that correct?
A. That's correct.
Q. What is that unit?
A. That unit supports FBI investigations. More notably, we support different field offices around the country. There's field offices in -- all over different states, and they primarily work on their own local issues. And occasionally, there will be special agents or computer scientists that need assistance with their cases either for technical reasons or staffing reasons, and we support them in that.
Q. Are you familiar with the FBI's cyber action team?
A. Yes, I am.
Q. Is that also referred to as the CAT team?
A. Yes, it is.

Q. What is the FBI's CAT team?
A. The CAT team is the FBI's incident-response fly team.
Q. You used two terms there. First, what's an incident response?
A. Incident response means if a company is compromised, if they have some kind of hack into their network, incident response is the operation where you go in and use threat risk and live system analysis to figure out what happened on the network.
Q. And you also said fly team?
A. Yes. A fly team essentially means that this team is ready to go at a moment's notice and goes all over the country and sometimes all over the world.
Q. Do you also support the FBI's CAT team?
A. Yes, I do.
Q. How do you do that?
A. I wrote the system on deployment, and as part of the technical analysis unit, when the bureau fly team -- it's essentially made up of special agents and computer scientists all over the country. When they're, like, on the on-call list, they can get sent out, and sometimes if they have too much evidence to analyze, they can send it back to us at headquarters, and we assist them with that.
Q. And you said sometimes you're deployed with the CAT team, is that correct?

A. That's correct.
Q. What do you mean deployed with the CAT team?
A. Deployed means I get to join them on the mission.
Q. Approximately how many times have you been deployed with the CAT team?
A. Five or so times.
Q. And generally how quickly is the CAT team deployed with cyber security?
A. It could be in a matter of hours to days, depending on the situation.
Q. Have you also helped develop forensic tools for the CAT team?
A. Yes, I do.
Q. Could you please explain?
A. Specifically, our team in the technical analysis unit, we do software development for the CAT team. Specifically, we've worked on multiple different ways to parse and triage forensic information from a network. Since the nature of incident response you're only going to be able to be on the ground for a few days, so you have to be able to process as much evidence as possible and get the best information that you can out of it; I support a development project that works to meet those goals.
Q. Putting the CAT team aside, in total, approximately how many investigations or cases have you assisted the FBI with?
A. Over my last six years or so with the bureau, between 50

and 100 or so.
Q. What types of investigations have you supported?
A. I've supported criminal cases, counterintelligence cases, other malware analysis-related cases, like nation-state malware, and some insider-threat cases.
Q. Generally, what was your role in those investigations?
A. As a computer forensic analyst.
Q. Have those investigations involved the analysis of computer networks?
A. Yes, many of them have.
Q. Approximately how many?
A. Dozens.
Q. What about the analysis of virtualized computers?
A. Yes.
Q. Approximately how many of the investigations involved virtualized computers?
A. Dozens of those as well.
Q. What about malware?
A. Slightly less. It depends on the situation. Most of the incident response-related deployments involved some sort of malware.
Q. And have you participated in investigations involving nation-state hacking?
A. I have.
MS. SHROFF: I'm sorry, your Honor. I had trouble

hearing.

THE COURT: Nation-state hacking.

MS. SHROFF: Sorry, your Honor.

THE COURT: That's OK.

A. Yes, I have.

Q. And what's nation-state hacking?

A. Nation state is just simply another term for a country or another entity that's significantly well funded and has access to a lot of resources.

Q. Approximately how many investigations involving nation-state hacking have you participated in?

A. Significantly less. Maybe five or less or so.

Q. What about investigations involving database reconstruction?

A. Very many. I'd say dozens.

Q. What do you mean by database reconstruction?

A. Pretty much all web services nowadays run databases. Even on your Windows machine you use at home, the web browsers use different databases, so those need to be analyzed for content.

Q. What about investigations involving insider threats?

A. I've worked very few, one that I can think of specifically.

Q. And what is an insider threat?

A. An insider threat is when you have an employee of a company or someone that works for a company and they're trusted with certain special information and they breach that trust and

either leak that information to someone else or sell it, something like that.

Q. And I think you said you've worked on one in particular?

A. Yes, I have.

Q. Which investigation is that?

A. The Harold Martin case, where he took information from the NSA.

Q. What was your role in that investigation?

A. We had an incident-response deployment that was --

MS. SHROFF: Your Honor, we have an objection. May we have a sidebar, please?

THE COURT: Yes.

MS. SHROFF: Thank you.

(Continued on next page)

(At sidebar)

MS. SHROFF: Your Honor, I'm sure the government can qualify this witness without eliciting information about a very recent case where there was a guilty verdict. The Harold Martin case is something that would be easily accessible to the jury. I mean, it's not like -- there's nothing about the Harold Martin case that has any co-relationship to this case, and to talk about a clear case where there's already a finding of guilt is just too prejudicial to Mr. Schulte.

MR. LAROCHE: We don't plan to elicit anything about the case itself.

MS. SHROFF: You may not.

MR. LAROCHE: We're not even talking about --

MS. SHROFF: But there is no reason to talk about another defendant. He can just say I worked on another case. He doesn't have to mention the lead case. He doesn't have to mention the NSA.

THE COURT: I think he can go into it by way of background, explaining what he did, why he's going to be an expert.

MS. SHROFF: Background is fine. He could say I worked on a case. He doesn't have to talk about the NSA, especially since this man also worked at the NSA. There's no reason.

THE COURT: He worked at the NSA? He was there as a

summer intern, correct?

MS. SHROFF: Yes, he was.

THE COURT: For three months? Two months?

MS. SHROFF: I'm just saying there's really no reason for him to talk about a specific defendant in a case. It's not necessary. It's prejudicial.

THE COURT: How much longer do you have with this?

MR. LAROCHE: We're over already.

THE COURT: Let's go.

(Continued on next page)

(In open court)

THE COURT: Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

Q. In addition to your work at MITRE, do you have any certifications in forensic analysis?

A. Yes, I do.

Q. What types of certification do you hold?

A. I have the GIAC, the certified forensic examiner certification.

Q. What is that?

A. It's the simple certification that covers everything from imaging hard drives and collecting evidence in a correct fashion to Windows forensics.

Q. Have you received any training on forensic analysis or cyber security?

A. Yes, I have.

Q. Approximately how many of those types of training have you received?

A. I've taken dozens of courses on the matter.

Q. What are some of the types of training that you've received?

A. Everything from programming courses to cyber security courses; instant-response courses, technical courses related to how the basic system internals of computers work, hardware hacking, things like that.

Q. Have you received any awards or recognition at MITRE for your case work?
A. Yes, I have.
Q. What are some of the awards that you've received?
A. I received a directors award related to the tool that I mentioned that we've developed for the instant-response team. That tool received the attorney general's award from the Department of Justice, so we were recognized in a similar fashion.

I've also received several other awards for my department just in support of cases that I've worked.
Q. You said the directors award?
A. No. The attorney general's award.
Q. Sorry. But I think you said you received the director's award. Is that correct?
A. Correct, from my company.
Q. And what is the directors award?
A. The directors award is one of the highest awards you can receive from our division.
Q. You mentioned the attorney general's award was related to that?
A. Yes, it was.
Q. What is that award?
A. That's a very highly respected award within the Department of Justice from the FBI.

Q. Other than from MITRE, have you received awards from anyone else for your case work?
A. Yes, I have.
Q. Who else gave you awards?
A. I received an award from the Polish national -- military counterintelligence service for a deployment that we did with them.
Q. Generally speaking, what did you receive that award for?
A. I received that award -- we helped them with an incident-response situation out of the country about a year ago.
Q. Did that assistance involve forensic analysis of computer networks?
A. Yes, it did.
MR. LAROCHE: Your Honor, the government would offer Mr. Leedom as an expert in digital forensics and computer science.
THE COURT: Any objection?
MS. SHROFF: We do have an objection, your Honor. But may I just ask two voir dire questions?
THE COURT: Yes.
VOIR DIRE EXAMINATION
BY MS. SHROFF:
Q. Sir, what is the highest level of education that you have in computer sciences?

A. I have a bachelor's of science in computer science.
Q. And is it fair to say that you do not have a master's of science in computer technology?
A. That is correct.
Q. And obviously, if you don't have a master's, you don't have a Ph.D., is that correct?
A. That's correct.
Q. And you have no specific knowledge or any expertise in any of the computer systems at CIA, correct?
A. Could you elaborate a little more?
Q. Well, before you were hired on this case, you were never part of the CIA, correct?
A. Correct.
Q. You had no access to any of their computers, correct?
A. That's not entirely accurate, but --
Q. OK. Tell us, sir. What was your access to CIA computers before you were retained on this case?
MR. LAROCHE: Objection.
THE COURT: Overruled.
A. Certain assets throughout the intelligence community are shared for intelligence purposes, so something -- news reporting, things like that.
Q. News reporting?
A. Things like that, yeah.
Q. What does that mean, news reporting?

A. Information on just different intelligence that's available for review.
Q. So they gave you access to DevLAN --
A. No.
Q. -- before you were retained for this case?
A. No.
Q. How about access to Confluence?
A. Not on their network, no.
Q. How about access to any of their computer networks?
A. Not on DevLAN, no.
Q. Did you receive any training about DevLAN before you arrived on this case?
A. No.
Q. Do you have any training whatsoever from your undergraduate college on DevLAN?
A. No, not for DevLAN specifically.
Q. I'm sorry?
A. Not for DevLAN specifically.
Q. OK. Do you have any network training on a network that was used or is in use at the CIA?
A. No, not for a specific network at the CIA.
Q. Right. So your only training about the topics on which you are about to testify is the training you got as a result of you preparing for testimony on this case, correct?
A. That's inaccurate.

Q. OK. Well, tell us what other thing you got to prepare for the testimony about the DevLAN network about which you are going to testify in this case.
A. During my undergraduate degree program and my past six years working with the bureau on operational-type engagements, I have significant experience working with both computer networks, varying companies that host different variety and types of computer networks and their basic operation. Those principles are the same to any network, even the networks at the CIA.
Q. OK. So your testimony sitting here today is the principles that you learned in college and then the principles that you learned from working on other networks, not at the CIA, essentially are the same principles that apply to the network that you're about to testify to, which is DevLAN. Is that correct? Did I correctly understand you?
A. That is correct.
Q. OK. So there isn't much of a difference between what you learned about other networks and you're able to apply what you learned about other networks to the DevLAN network about which you are going to testify, correct?
A. That's correct.
Q. So basically the principles about how general networks work and how the DevLAN network works are essentially the same, correct?

A. That's accurate, yes.
Q. It's accurate, right?
A. Yes.
MS. SHROFF: OK. Could I have just one second, your Honor?
THE COURT: Yes.
MS. SHROFF: Thank you.
Your Honor, given the fact that the witness has testified that his knowledge of the DevLAN network is informed by his knowledge of other non-DevLAN, non-CIA networks, we withdraw our objection to him becoming an expert.
THE COURT: You withdraw your objection?
MS. SHROFF: I do.
THE COURT: He's recognized as an expert then.
MS. SHROFF: Thank you very much, your Honor, for the voir dire.
THE COURT: You're welcome.
BY MR. LAROCHE:
Q. So let's start there. Did there come a time when you became involved in the investigation of the DevLAN network?
A. Yes, there was.
Q. And did that involve the Vault 7 and Vault 8 disclosures?
A. Yes, it did.
Q. What is Vault 7 and Vault 8?
A. To my knowledge, Vault 7 and Vault 8 were leaks of

classified information from the CIA; specifically, the DevLAN network.

Q. And when did you become involved in the Vault 7 and Vault 8 investigations?

A. I personally became involved in the investigation, I believe it was late March 2017, maybe early April.

Q. Based on your participation in that investigation, did you develop an understanding as to whether the information in Vault 7 and Vault 8 was stored on any particular computer network?

A. Yes, I did.

Q. What computer network was that?

A. It was stored on the DevLAN network.

Q. And is that a CIA computer network?

A. Yes, it is.

Q. Now, before the Vault 7 and Vault 8 disclosures, did you have access to DevLAN?

A. No, I did not.

Q. Why not?

A. It was a classified internal agency network.

Q. What were your responsibilities in connection with the Vault 7 and Vault 8 investigation?

A. Primarily, we had sort of incident response-type deployment to the agency to assist them with investigating what happened.

Q. As part of your responsibilities, have you also reviewed network diagrams and documentation of the DevLAN network?

A. To some extent, yes, I have.
Q. And I think you said that your first role was incident response. Is that correct?
A. That's correct.
Q. Could you just explain generally what you mean by that?
A. We were there to assist in trying to figure out if there potentially were any, like, nation-state hacking attempts, any malware active on the network, things like that.
Q. Did that role transition over time?
A. Yes, it did.
Q. How did it transition?
A. As we were supporting and became more knowledgeable about the network, my role transitioned into more of a computer scientist role supporting the investigation itself.
Q. Now, as part of your responsibilities and participation in this investigation, did you examine forensic files and data from the DevLAN network?
A. Yes, I did.
Q. Did that include reviewing the computer the defendant used to access DevLAN while working at the CIA?
A. Yes, it did.
Q. Did it also include reviewing servers connected to DevLAN?
A. Yes, it did.
Q. Approximately how much time have you spent over the past two and a half-plus years reviewing those materials?

A. Countless hours.
Q. Have you formed an opinion as to some of the defendant's activities on the DevLAN network in April of 2016?
A. Yes, I have.
Q. I want to focus your attention on April 20, 2016. Have you reached an opinion as to the defendant's activities on the DevLAN network that day?
A. Yes, I have.
Q. What are some of the opinions that you've reached about the defendant's activities on April 20, 2016?
A. On April 20, 2016, the defendant accessed the Confluence virtual machine, which was running on the OSB ESXi server. He then reverted that virtual machine to the 4/16 backup that you've heard about ISB having had made before they changed the passwords. That backup gave him access to the machine again after the passwords were changed. During that time the machine stayed in a reverted state for a little over an hour, and the defendant copied the Confluence backups from the Altabackup server.

Also during that time, the defendant deleted many log files both on the ESXi server itself and on the virtual machine by reverting to the previous snapshot and deleting it.
Q. Now, as part of your role in this investigation, did you also review the Vault 7 and Vault 8 disclosures that were posted by WikiLeaks?

A. Yes, I have.
Q. I want to focus on the initial disclosure, made on March 7, 2017.
A. Yes.
Q. Do you have an understanding about where that information came from on the DevLAN network?
A. Yes. That was Confluence data.
Q. And how do you know that?
A. I reviewed it.
Q. How much of Confluence, approximately, was disclosed by WikiLeaks on March 7, 2017?
A. All of it.
Q. Based on your analysis in this case, have you reached an opinion as to what Confluence files were provided to WikiLeaks?
A. Yes, I have.
Q. What is your opinion?
A. It was the, those March 3 backup files.
MR. LAROCHE: Ms. Hurst, can you please show the witness, the parties and the Court what's been marked as Government Exhibit 1703, please.
Q. Mr. Leedom, do you see that on your screen right now?
A. Yes, I do.
Q. Do you recognize this?
A. Yes, I do.
Q. What is it?

A. It's a presentation that I've put together to help explain this.

Q. And did you assist in preparing this presentation?

A. Yes, I was.

Q. And does this summarize some of the exhibits you reviewed as part of this case?

A. Yes, it does.

Q. Will it help you explain your opinions as you testify today?

A. Yes, it will.

MR. LAROCHE: Your Honor, the government would offer Government Exhibit 1703 as a demonstrative.

THE COURT: Ms. Shroff.

MS. SHROFF: Your Honor, I just remind the Court that we have a pending objection.

THE COURT: Yes.

MS. SHROFF: Subject to that objection --

THE COURT: 1703 is received in evidence.

MR. LAROCHE: Thank you, your Honor.

(Government Exhibit 1703 received in evidence)

MR. LAROCHE: If we could publish that to the jury.

Q. Now, Mr. Leedom, is your presentation broken up into different parts today?

A. Yes, it is.

Q. And what is the first part?

A. This is a basic overview of the DevLAN network, covering some of the basic features, basic configurations, things like that.

Q. What do you mean by basic configurations?

A. Tried to present this in a way that's more towards the layman and doesn't include, like, for example, complex diagrams from SSPs, things like that.

MR. LAROCHE: Let's go through the part 1 DevLAN overview, if we could go to the next slide, please.

Q. This slide is titled "networking overview"?

A. Yes.

Q. And the first sub-bullet is firewalls?

A. Uh-huh.

Q. What are firewalls?

A. In its simplest term, firewall is a physical piece of hardware that's on a network that limits activities on those networks between different machines.

Q. And the next sub-bullet is switches?

A. Yes.

Q. What are those?

A. A switch is one way to connect computers to each other, essentially.

Q. And finally, routers?

A. Routers are ways to connect, that you would connect multiple different networks together.

MR. LAROCHE: Let's go to the next slide.
Q. What is this slide showing?
A. This is a simple diagram of how DevLAN was laid out.
Q. And if you could, just start at the left with the box that starts DevLAN and just explain to the jury what each of the boxes are meant to represent.
A. Yes. So the box on the left, see if I can draw, this is essentially a switch that's just representing the different connections between all the computers on the DevLAN network. There was a firewall that was limiting access, certain accesses to what we've seen in the full version of this exhibit, the Hickok network here, in the gray. And then we have the COG network on the right over here.
MR. LAROCHE: Thank you. Let's go to the next slide, please.
Q. Slide 4 is titled "operating systems"?
A. Yes.
Q. Generally, what's an operating system?
A. An operating system is the software that runs on top of the hardware on your computer.
Q. What types of operating systems were run on DevLAN?
A. DevLAN had three major types, which is essentially all of the available operating systems. The first is Linux, which we've seen here. It's a very popular open-source operating system. You can access it from either a graphical user

interface, or most commonly, as we see in this case, it's on servers that were running on the network.

There's also the Windows operating system, which is developed by Microsoft, which has a graphical user interface that many of you have seen. And MacOS.

Q. What is MacOS?

A. MacOS is developed by Apple, similar graphical user interface operating system.

MR. LAROCHE: Let's go to the next slide, slide 5, please.

THE WITNESS: Yes.

Q. What is this slide meant to convey?

A. I just want to show here the different types of operating systems that were in place on different parts of network. So, most of our Windows machines and potentially Mac machines would be located in the DevLAN user section, so different users would have different machines based on the type of work they were doing. Like, for example, if you were working on tools related to MacOS, you would have probably a Mac machine; same for Windows and also Linux there.

The Active Directory server, which we'll just represent in this little box here, that maintained, like, access controls for the network. That's a Windows server running a version of Microsoft Windows.

And then the management servers across the network, like

ESXi server, Stash server, I believe the Hickok server, these were Linux-based machines.

MR. LAROCHE: Thank you. We'll go to the next slide, please.

Q. Slide 6 is titled "virtualization"?

A. Yes.

Q. What's virtualization?

A. Virtualization in respect to computers is essentially a way of running a computer inside of a computer.

Q. And the first sub-bullet here is a virtual machine?

A. Yes.

Q. What's that?

A. So, A virtual machine, like I said, is a way to run a computer inside of a computer. This isn't limited to just running on servers. You can do this at home on your laptop if you want with free software. Typically, in a production environment, this is used to help both aid development and have higher uptime.

Q. You said production environment?

A. Yes.

Q. What i's that?

A. When I say production environment, I typically mean in some kind of server infrastructure for machines that are meant to be accessed by multiple users and are meant to be relatively stable so that they provide a service that, you know, doesn't

get turned off every night when you go home.
Q. And you also used the term "uptime"?
A. Yes.
Q. What does that term refer to?
A. Uptime just refers to how long a service has been running. So, if you say a service has high uptime, it means it doesn't crash often, it maintains relatively stable.
Q. The next sub-bullet is ESXi servers?
A. Yes.
Q. What are those?
A. ESXi is a, what we call a hypervisor. It's a type of operating system, a type of Linux operating system that is developed by a company called VMware. And it's used, its sole purpose is to host virtual machines.
Q. The next sub-bullet is VMware vSphere?
A. Yes.
Q. What does that refer to?
A. VMware vSphere is a way to manage virtual machines on this ESXi server.
Q. What do you mean by a way to manage virtual machines?
A. So, what you would do to -- if you wanted to access a virtual machine, one way you could do it is by launching the vSphere application either through double-clicking the application on your Windows machine or navigating to a web service that provides the same level of access.

You can go into that application, view a list of all the machines running on the server. You can actually what we would refer to, the term is "shelling in" to the machine, which is you click a little -- a little box, and it would actually give you, like, a little window into that computer where you can move the mouse and things like that, if it had a graphical user interface.

It's just a way to manage those machines. You could create snapshots, revert snapshots, add more memory to a machine, more hard drive space, things like that.

Q. And then finally, VMware vCenter?

A. Yes.

Q. What does that refer to?

A. Yeah, vCenter is a management application that goes kind of along with vSphere and ESXi. It just helps add access to the management part of the ESXi server.

MR. LAROCHE: Let's go to the next slide, slide 7.

Q. This is entitled "Atlassian suite." What is Atlassian?

A. Atlassian is the name of a company.

Q. And did DevLAN run certain Atlassian services?

A. Yes, they did.

Q. What services?

A. They ran than mainly five Atlassian services that are listed here on the slide.

Q. Can you give a brief description of each of those services?

A. Yes.

so, Confluence, as we've heard -- it's a Wiki. It's used for user collaboration, so if you want to share information with other users, essentially just a place to post information. Each user has their own specific page. Users can make other pages for other users to see. Users can restrict pages from other users, things like that.

Stash, Bamboo and Jira kind of go together. This is a software development package. So, as a software developer, you write code, so this code needs to be stored in had a way that can both be, you know, backed up and have different revisions and allow multiple people to contribute to the project.

Stash allows you, Stash provides some services to support some of the different types of software we call version control software. In this specific case, the type of version control is called Git. And it essentially just allows multiple users on the system to have access to these source-code repositories or projects and contribute to them, make changes and do it in a stateful way.

This ties into Bamboo. Bamboo is what we call in the software development industry a continuous integration platform. Essentially what you do is if you're writing your code and you feel like you've done for the day, maybe you've added a feature, like a new button on a web page, you will commit your code and it will go up to Stash and be saved. And

then that code can get transferred automatically into Bamboo, which will run it for you and tell you if it's working like you intended to or if there were any errors. That's what that's for.

Q. What about Jira?

A. So, Jira is -- it's an issue tracker. I think we've heard it referred to as, like, a help desk. So, if you have users that are using your software or even other developers that are working on your software, you want to keep track of different, maybe, problems you're having, what you plan to fix in the next few months, feature requests, things like that.

Q. And finally, Crowd?

A. Crowd is an integration to the Atlassian suite of programs that is designed to integrate mainly with Windows Active Directory, which manages all of the user accounts on a network. It essentially allows you to kind of plug it into that, and it can handle interfacing those permissions with the rest of the Atlassian products.

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

Q. Does this slide show where the various Atlassian services were being run on DevLAN?

A. Yes, it does.

Q. And can you explain that?

A. Yes. So, Confluence and Bamboo, here, are both virtual machines running on the ESXi server.

Stash and Crowd were both running on a physical Stash server. And then Jira was running on a physical Hickok server.

MR. LAROCHE: If we could just zoom in on the ESXi server, please, on the top left there.

Q. And you said Confluence and Bamboo were running as virtual machines?

A. That's correct.

Q. Is that different than running directly on the server?

A. Yes, it is. It's significantly different.

Q. Just explain the difference there.

A. So, a virtual machine is essentially its own self-contained little personalized computer. You can push a pause button on it and it will freeze everything that's happening. You can restart it. You can turn it on and off like you would a normal computer. You can define how much memory it gets, how much CPU time it gets, how big the hard drive is.

We've heard about snapshots. You can take a snapshot, which is essentially like a backup in time of how the server was, so if you're about to make a drastic change and it went poorly, you could revert back to that and have the machine back where it was when you accessed it.

These are just different computers that are all virtualized for ease of use.

(Continued on next page)

Q. Then on the right side of this box, there's developmental VMs?

A. Yes.

Q. What is that meant to refer to?

A. There were, so this is a development network, particularly for offensive capabilities, you need a way to test these tools, some of them require networked computers. You can generate an entire, you know, fake computer network inside of a cluster of virtual machines on the server to test your tools. You can install specialized operating systems and things for the targets that you're trying to attack, and it's just how you use the virtual machines in that way.

Q. Let's go to the next slide. Slide nine. It is titled "file storage." And the first is NetApp server. What's that?

A. A NetApp server is essentially a big NAS which is defined as network attached storage. It is essentially a server that sits in the server room and has a ton of hard drives connected to it to store their data.

Q. And the next sub-bullet is "backups."

A. Yes.

Q. What are backups?

A. Backups are, in this case referring to backups for the Atlassian suite. They're copies of data that you would need to restore a server, should the server ever, ever, you know, completely crash beyond being able to recover it. It would be

all the files you need to restore that to its state as of the time you took the backup.

Q. Let's go to the next slide, please. Did DevLAN have a NetApp server?

A. Yes it did.

Q. If we can just zoom in on that in the bottom middle of the screen, please. What was the NetApp server used for on DevLAN?

A. Primarily three things. There were user home directories that individuals users had to store their personal data. Just to back it up in case, you know, their machine went down or whatever happened. There's the Altabackup share, which was used to talk to the Atlassian services and store their backup files. And there was a method for delivering completed tools on the network in another share as well.

Q. Let's go to the next slide. Slide 11 is titled "access controls."

A. Yes.

Q. Generally, what are access controls?

A. Access controls are how you limit the operations of different users on the network.

Q. And first bullet here is "domain controller"?

A. Yes.

Q. What's that?

A. As I mentioned previously, the domain controller on DevLAN was a type of technology called Windows Active Directory. It's

from Microsoft. It basically has a bunch of different user accounts and different roles for those users. You may have a user that's domain admin. That means they can do pretty much anything on the network. You may have users which are just developers, which might have different types of permissions.

Q. The next sub-bullet is "user authentication."

A. Yes.

Q. What does that refer to?

A. Many applications like Crowd interface with this domain controller over a protocol called LDAP. It is just a way for the computers to talk to each other and make sure that users are using the -- that users are enforced with authentication.

Q. And the third bullet is "secure shell."

A. Yes.

Q. And defined as SSH?

A. Correct.

Q. What does that refer to?

A. SSH is a way to interact and remote into machines using the command line. When I say command line, I mean, if you think back to the days before computers had like a mouse and like icons to click on. It was just a keyboard and a terminal. That's essentially what the command line is.

I think you've heard to it referred to earlier in these proceedings as like the DOS command prompt from back in the day.

It is essentially a way you type on the terminal and can connect to different remote service -- different computers remotely. You can do this with a user name or a password. Or you can use what's called a public private key pair. These are essentially just large numbers that are related mathematically. And if you wanted to access a server with a public private key pair, you'd first need to generate a key pair that's your own. And then you receive two parts, you have a private key, which you keep private and keep to yourself. And you have a public key. And you can place this public key on servers that you want to have access to, and it knows how to ask you when you go to log into it for your private key, and that's how you authenticate to the server.

Q. Are they also referred to as SSH keys?

A. Yes, they are, that's another name for them.

Q. The last bullet on here is "file share permissions."

A. Yes.

Q. What does that refer to?

A. Permissions on the file share could be enforced through LDAP, which is the Active Directory server, or through other means.

Q. Let's go to the next slide. As part of your review in this case, have you attempted to determine approximately how many DevLAN users there were in April of 2016?

A. Yes, I have.

Q. How did you go about doing that?
A. We received information from a backup copy of the domain controller. And all of the, like, all of the user accounts and computer accounts were dumped out of that into a big spreadsheet, and I analyzed that to determine how many users were active. And it's about 200 users.
Q. As of when?
A. As of April 2016.
Q. Let's go to the next slide. Now, earlier we talked about the home folders on the NetApp; do you recall that?
A. Yes.
Q. Slide 13 shows Government Exhibit 1207-60. Where is that exhibit from?
A. This is from the NetApp server.
Q. What part of the NetApp server is this showing?
A. This is where all the home folders were on that share. So this is where an individual user would store their data if they wanted to back it up, for example.
Q. If we could just zoom in on the exhibit, please. Actually, can we just zoom in on the top maybe quarter there.

Just to start at the top. There is an offline_vault.

A. Yes.
Q. You see that? What's that refer to?
A. From my understanding, the DevLAN network had like two NetApp machines running. Typically in an enterprise network,

you have backups of sometimes even your backups, for both fail over, and in the case of a network like DevLAN where you were potentially developing malicious tools if something accidently maybe deleted the files from your file server, you would need a way to come back to that.

From what I understand from participating in the investigation, after a certain amount of time, I'm not sure if it was weekly or daily, they would do a mirror from the main NetApp server on to the offline vault which was sitting right next to it in the server room. And that's what is restored here.

Q. Zoom out again. What are each of these folders reflecting?

A. These are individual user folders on the NetApp server.

Q. Let's go to the next slide, please. This slide is titled "administrators."

A. Yes.

Q. Were there different types of administrators over the DevLAN network?

A. Yes, there were.

Q. Generally, when you hear the term "administrator," what do you understand that to refer to?

A. An administrator is someone who has access either to providing other users access to a machine or maintain the machine itself.

Q. Let's go to the next slide, please. I want to focus on two

types of administrators on DevLAN. Were there Atlassian administrators?

A. Yes, there were.

Q. What are those administrators?

A. Atlassian administrators had access to things like the Atlassian web services. So for Confluence, for example, they would be able to add and remove different users permission for pages for Stash, add and remove users from projects, perform basic administrative duties. In some cases if a service was broken, they could go into the virtual machine for the Atlassian server and fix things.

Q. What about server administrators.

A. Server administrators are kind of your like tiptop level of administrators. These administrators will have access to the servers themselves, they'll be able to go in and fix problems, any hardware changes, things like that you'd have to make to a server, types of things we are talking about.

Q. Let's go to the next slide, please. You talked about an ESXi server that was running Confluence and Bamboo?

A. Yes, I did.

Q. As of April 20, 2016, who did that server belong to?

A. April 20, that server still belonged to OSB.

Q. We're showing you Government Exhibit 1202-5. Where is this exhibit from?

A. This is from the Confluence web server.

Q. What is it showing?
A. This shows information about how to connect to different virtual machines on the ESXi server.
Q. If we can just zoom in on the bottom quarter starting with infrastructure VMs. You see the first line that starts osb.devlan.net?
A. Yes, I do.
Q. What does that name refer to?
A. This is the ESXi server itself. It is the host name for the server.
Q. As we go over, there is a user name column with root.
A. Yes.
Q. What does root refer to?
A. Root in the Linux world is essentially another name for the administrator account.
Q. Then next to that there is a password?
A. Yes.
Q. What's that password for?
A. That's the password to log into the root account for the ESXi server.
Q. On the right there is "additional notes."
A. Yes.
Q. It says "Connect via vCenter" then there is an @ and an address?
A. Yes.

Q. What's vCenter?
A. VCenter, this is the web application. It behaves similarly to vSphere. It lets you go into the server and access the virtual machines, create new ones, delete them, things like that.
Q. We can pull that back out, please. The next slide, let's go to the next slide. Slide 17.
I want to talk for a moment about access to the final products.
A. Yes.
Q. Again, where are the final products located?
A. So the final products is a share that's on the NetApp server for tool delivery. I'll circle it here.
Q. Let's go to the next slide. This slide has Government Exhibit 1207-49. Where is this exhibit from?
A. This is from the NetApp server.
Q. What is it showing?
A. This is showing one of the shares, the EDG main share from the NetApp.
Q. You see there a folder at the bottom, "source code and binary gold copies"?
A. Yes.
Q. What are those?
A. These are the delivered completed tools from the work at EDG.

Q. As part of your investigation, did you determine the controls or file permissions on that folder?
A. Yes, I did.
Q. Let's go to the next slide. Slide 19 has Government Exhibit 1207-50. You see that?
A. Yes, I do.
Q. What is this showing?
A. This is, if you would essentially right click that folder on Windows Explorer and click "properties," this is the screen that would come up.
Q. What types of things do the properties tell you about a folder?
A. It tells you the size of the folder, the number of files on the folder, the different attributes for the folder, and in the security tab you can see what people have access to the folder.
Q. You see the size there?
A. Yes, I do.
Q. What's the size of this folder?
A. It's a little over one terabyte.
Q. Let's go to the next slide, please. This slide, slide 20 shows you Government Exhibit 1207-52. What is that exhibit?
A. So, this is, if you start digging down through those properties, these are the different user groups that would be on the domain controller for different users that would have access to that folder.

Q. Did the defendant belong to any of these groups?
A. No, he did not.
Q. Would the defendant have been able to copy the gold source folders?
A. No, he would not have had access to it with his DevLAN account.
Q. Let's go to the next slide, please. I want to talk for a moment about access to the NetApp backups or Altabackups.
A. Yes.
Q. So let's go to the next slide. This is the government Exhibit 1207-49 again. We just saw this a second ago. Is that correct?
A. Yes, we did.
Q. Where is the Altabackups folder on this slide?
A. It's not on this slide.
Q. Why not?
A. It was a separate share. It wasn't in the same share as these folders, it was separate.
Q. You said "separate share"?
A. Yes.
Q. What do you mean by that?
A. On the NetApp server itself, you can set up, like, separate volumes that are shared in different ways that can have different permissions and different accesses. Altabackup was a separate one of those.

Q. Let's go to the next slide, on slide 23, and there is Government Exhibit 1207-8. You see that?

A. Yes.

Q. Where is this exhibit from?

A. This exhibit comes from the Confluence virtual machine that was running on the ESXi server. This is specifically from the snapshot, that BK 4-16-2016 snapshot.

Q. If we can zoom in at the bottom on the highlighted text. What does this text reflect?

A. So, this file in the exhibit is a file called FStab that's on the server. This is where you would make an entry if you wanted the server to automatically mount a folder location. Like a remote folder location on the server every time it's rebooted or you run the mount command.

Q. So, is this a mount point?

A. Yes, it's another way to refer to it.

Q. What's a mount point?

A. A mount point is a point on the server where you can access an external resource. If we go through this piece by piece. The first part of this, this is just saying what server you want to connect to and what share or folder on that server you want to connect. In this case it's the 10.3.1.70/Altabackup.

Second part of this is the local folder on the server itself where you want to tie that network location to.

The next part of this says what type of, like, file

system protocol you are going to use to connect to it. In this case it's NFS.

Then the rest of this are permissions to the mount command.

Q. On the left there is 10.3.1.70?

A. Yes.

Q. What is that?

A. That's the IP address of the NetApp server.

Q. Where is this mount point located?

A. On the NetApp server, it's one of the volumes on the NetApp server. Locally it's in this folder that's called /mount/Altabackup.

Q. I think you said it was mounted to a server; is that correct?

A. Yes.

Q. What server are you referring to?

A. This is from the Confluence virtual machine.

Q. When you referred to a Confluence virtual machine, do you also sometimes refer to it as a Confluence server?

A. Yes, I do.

Q. Why do you refer to it like that?

A. A virtual machine can be -- typically the word "server" is reserved for machines that are, have a significant amount of resources available to them. Or a machine that's just providing some kind of, like, a division level resource or a

resource that multiple people are accessing. That's just what a server is. So since it's hosting a service called Confluence and a lot of people are using it, that's why we call it a server.

Q. How do you access the mount point on a Confluence virtual machine?

A. You would navigate to it in the terminal.

Q. Could a regular user access that mount point?

A. No. Regular users on DevLAN only had access to the Confluence web service, which wouldn't display any kinds of folders or files from the server itself.

Q. So, what would you have to be logged into to access this mount point?

A. You would have to be logged into the administrative account to manage the server.

Q. How would you log in that way?

A. You could either use vSphere to go in and click on the virtual machine and open up a shell to that server. And then you'd have to enter the user name and password for the administrative account on the server. Or you could use the SSH utility and a public private key to log into the server. Or SSH with a password to log into the server.

Q. Were there other mount points for other Atlassian services on DevLAN?

A. Yes, there were. They were all contained in inside of

Altabackup.

Q. Where were those mount points located for those services?

A. They were mounted on the other Atlassian servers.

Q. What privileges would you have needed to get to those mount points?

A. The same as Confluence, administrative privileges to access the actual underlying server that could see those folders.

Q. Let's go to the next slide. Slide 24 is showing Government Exhibit 1207-36. Where is this exhibit from?

A. This is from the NetApp server.

Q. What's it showing?

A. These are different folders that were in the Altabackup folder.

Q. On the last slide we were looking at a mount point on a Confluence virtual machine; is that right?

A. Yes.

Q. If you had access to that mount point, could you get to the Altabackups?

A. Yes, you could.

Q. That was on a Confluence virtual machine; is that right?

A. That's correct.

Q. Would that limit you to the Confluence backups?

A. No, you'd have access to the other backups as well.

Q. Let's go to the next slide, please. This slide has two exhibits, Government Exhibit 1207-27 and 1207-30. Where are

those exhibits from?
A. These are from the Confluence backup folder on the Altabackup.
Q. Let's just zoom in there on the left exhibit, please. Can you tell us, there is a type in the middle there. Sql file?
A. Yes.
Q. What types of files are these?
A. So, sql, it stands for structured query language. It is a type of database file. Specifically, the type of database that the Confluence server used to store its information.
Q. And then let's start at the left, there is a name column which is the name of the backup. Is that right?
A. That's correct.
Q. Approximately how often were the Confluence -- withdrawn.
How often was Confluence backed up?
A. It was backed up daily.
Q. How do you know that from this slide?
A. We can see from the time stamps of the backups that they were, they finished backing up just before 6:30 every morning.
Q. You see there is a date modified column?
A. Yes.
Q. What is that?
A. This is the time that the file was last written to. Otherwise, the contents of the file were last changed.
Q. You see next to type there is a size column?

A. Yes.
Q. Approximately how large are these sql files?
A. They are about 400 megabytes apiece.
Q. What about date accessed, what's that?
A. Date accessed is the last time the file was accessed. In this particular instance, based on what's changed here, this would have been the last time the database was -- when it was pushed to the backup server. Read operations, copy operations, modifying a file. Just about anything you do to a file will update that date accessed time.
Q. What about date created, what's that?
A. That's the time that the file was created.
Q. Let's zoom out, please. And then zoom in -- sorry, last slide, still. And zoom in on the other side, please.

This in the type has winRAR archive; do you see that?

A. Yes.
Q. What types of files are these?
A. So, these are, they are zip files. When you have a -- most of the Atlassian services, to make a complete backup of them, you would need a copy of the database, and you would also need a copy of what we see here is like the home folder for the individual service. This home folder for Confluence specifically stores things like server configuration information, how the server is supposed to run. Things like this is where your page attachments would be stored. So, if on

Confluence you attached a picture to a page, it would be stored in this home folder. And you need both pieces to be able to restore the server to its state, if you are going to use it as a backup.

Q. We can go to the next slide, please. The title of this slide is "Some Confluence Backup Files As Of July 27, 2016." Do you see that?

A. Yes.

Q. What's that meant to convey?

A. This is just like a snip of some data from, like, the previous slide.

Q. Then, let's take a look just on the top starting at the top Exhibit 1207-27, please. Just zoom in, I'm sorry.

Have you reviewed the backup files for Confluence that are contained in the Altabackups folder?

A. Yes, I have.

Q. Has there been any time when you've seen a different date accessed time than date modified and date created?

A. Only in one instance.

Q. Does that appear on this slide?

A. Yes, it does.

Q. Can you explain this?

A. This for this March 3 backup, which I'll attempt to -- there we go. Here we'd seen this file was accessed on 4/20/2016 at 5:42 p.m.

Q. Let's zoom in and zoom in on the bottom exhibit, please. Same question. Do you see a different date accessed and date modified and date created?

A. Yes, I do. It is for the March 3 backup, again, and it's for 4/20/2016 at 5:43 p.m.

Q. Let's go to the next slide. Have you also reviewed the Stash backups?

A. Yes, I have.

Q. And the title of this is "Earliest Available Stash Backup Files As Of July 27, 2016." Do you see that?

A. Yes.

Q. What's that meant to convey?

A. This is just to show that when we arrived on site, the earliest backups from Stash we were able to get were from May 1st, 2016.

Q. Why is that?

A. If you look to the right on the size column, you'll notice that these are very large. Like 210 gigabytes compressed. Since this contained all the project source code, these were really big. So, from like a system administration standpoint, to save on space, it's not hard to imagine that these were the ones that were removed first, just for storage purposes.

MS. SHROFF: Objection to the imagination.

THE COURT: It is a phrase of speech. Objection is overruled.

Q. Let's go to the next slide, please. This slide is titled "Navigating to the Altabackups." And Government Exhibit 1203-13 appears on this slide.

First, where is this exhibit from?

A. So, this exhibit comes from a virtual machine on the defendant's DevLAN computer. This is some activity from a session that was recovered from what we call unallocated space from inside that virtual machine.

Q. Let's pause there and just talk about first the virtual machine part of that.

A. Yes.

Q. You said it's from a virtual machine on the defendant's DevLAN computer?

A. That's correct.

Q. What does that mean?

A. Like I mentioned earlier, you don't have to just run a virtual machine on a server. You can run it on your own computer. In this case, we can see that this was a version Linux called Ubuntu which is one of the more popular free Linux distributions. It has a graphical user interface and things like that.

Inside of this virtual machine we were able to recover what's essentially deleted data. And of that data is part of one of the sessions.

Q. You said this is from the unallocated space of that virtual

machine?
A. Correct.
Q. Generally, what is unallocated space?
A. So, on most modern file systems, on computers, when you click the delete key on a file, it doesn't go and actually erase all the contents of that file. It, depending on different types of file systems it behaves a little differently. But in most cases, it essentially just marks that file as deleted. And but the actual clusters or blocks on disc where that file was originally stored still contain that data.

So, as a forensic analyst, we can go in and look at those unused blocks or clusters and recover the original data that used to be there.
Q. You see on the bottom left of this slide there's E0001. Do you see that?
A. Yes.
Q. Can you circle that?
A. Yes, I can.
Q. What does that refer to?
A. That's an evidence tracking number that was used just to identify the defendant's DevLAN work station.
Q. Is that tracking number E0001?
A. Yes it is.
Q. Next to that there is a dash Ubuntu X64.
A. Yes.

Q. What does that refer to?
A. This is the virtual machine on the defendant's DevLAN work station. Like I mentioned before, it's an Ubuntu Linux operating system. The X64 just means it is a 64-bit variant.
Q. Next to that is "unallocated space log."
A. Yes.
Q. What does that refer to?
A. This refers to the data that we recovered from unallocated space inside of that virtual machine.
Q. So let's just look at this log. Just so we can zoom in on the top quarter, please. Start at the top left.
A. Yes.
Q. Can you walk us through what that first line is showing.
A. This first line shows what appears to be the bottom of a FStab file, which we saw a few slides ago. This is from an actual shell session, so if you were typing in the terminal, this is the output and types of commands you would see.

So, same as the FStab file, before we see the IP address for the Altabackup server, the share name, the place it would be mounted locally, and the file system type.

Q. What about the next line.
A. So this next line I'll go through it piece by piece so we can talk about it.

So this root@dev01. Root is the user that you are currently signed into in this session. And then the @dev01 is

the host name of the computer that you're logged into. Dev01 in this case is the Stash server. This little tilde here is a representation of the home directory for that root user that you're in. And then the command that's to the right of this, this CD/mount/altabackup, CD is a command in Linux which stands for change directory. So, all this is saying is, please change my directory to the directory location/mount/altabackup.

Q. What about the next line?

A. So this shows that that command that was previously successful, because now instead of this little tilde we have this notifying us we are in a folder called Altabackup. Then the command that's run here is the LS command, which stands for list, which just asks the computer to show a list of files in that directory.

Q. Then there is a line below that.

A. Yes.

Q. What's that show?

A. This is just showing the result of that list command. So, as you've seen previously in the other slides, inside the Altabackup there is folders for Bamboo, Confluence, Crowd, Jira, Stash, and then that test.txt file.

Q. Then below that?

A. Below that, this is changing the directory to the Stash folder inside of Altabackup.

Q. Then finally the last line here?

A. Then the last line just listing the contents of that Stash folder.

Q. If we could zoom out. You see the output of that list command?

A. Yes, I do.

Q. Where is it?

A. It's below here. I'll draw an arrow. This is just the backup files for Stash.

Q. Let's go to the next slide, please. This is just titled "DevLAN Network Documentation." Generally, what is network documentation?

A. Network documentation is paperwork that just displays how the network is organized, what certain data protections or protocols are in place on the network. How different the network -- you might hear it called network topology, so different router switches, computers, how things are plugged together.

Q. What are some of the network documents you reviewed in this case?

A. I've reviewed some of the SSPs, which are like the security paperwork that said what restrictions would be on the network and how it was laid out.

Q. Are there any portions of those network documents that are incorrect?

A. There are some incorrect portions.

Q. Can you give us an example?
A. One example is I know at least some IP addresses from some of the SSPs didn't quite match up to what I saw on the network when we were reviewing it.
Q. Let's go to the next slide, please. Is the second part of your presentation related to the defendant's DevLAN computer?
A. Yes, it is.
Q. Let's talk about that computer. The first slide that we're looking at, slide 31, is titled "ownership" and it shows Government Exhibit 1202-2.
A. Yes.
Q. Where is this exhibit from?
A. This exhibit is from the -- so the DevLAN's computer was a Windows workstation. And Windows has something called the Windows Registry. It is essentially like a database where Windows stores information about the computer.

In this case, we're looking one of the keys in the registry. That just says who the registered owner of that machine is. This is something that's configurable. Typically when you would install Windows on a computer, it will ask you what's your name. That's what this is.

Q. You see the top line refers to registered owner Schuljo?
A. Yes.
Q. What's that?
A. That's the defendant's user name. Josh Schulte. Just kind

of, yeah.

Q. Let's go to the next slide, please, slide 32. Showing Government Exhibit 1202-2.

A. Yes.

Q. Where is this exhibit from?

A. This is also from the registry on the defendant's DevLAN workstation. This is specifically from what we call our registry hive. A registry file called SAM, which stands for Security Account Manager. This shows what user accounts were available to access that computer and the number of log-ins that those user accounts had.

So if we take a look at the Schuljo account, we can see there were 1343 log-ins to that computer. So it's clear, this just shows it was the defendant's computer.

Q. And when is the last log-in?

A. The last log-on date was October 27, 2016.

Q. Let's go to the next slide, please. This slide is titled "Workstation IP Address is 10.3.2.165."

A. Yes.

Q. Just generally, what's an IP address?

A. An IP address is the way that computers talk to each other. It's like an addressing system. It's typically not used in normal conversation. You use something called a host name. And there is a service that runs on like the Active Directory server that takes a host name, which we'll discuss here, and

converts that to an IP address. So you don't have to remember the string of numbers, you can just say what the plain text host name is.

Q. This is showing Government Exhibit 1203-48. What is this exhibit?

A. This exhibit is an excerpt from a log file in VMware, just showing the host name and IP address of the defendant's DevLAN workstation as of April 12, 2016.

Q. What's a host name?

A. A host name is a human readable name for a computer. Essentially, the name of the computer.

Q. How is a host name set?

A. It's configurable. You can enter a command to change it or you can change it.

Q. Who does that?

A. The owner of the computer.

Q. What's the host name of this computer?

A. The host name for this computer is KingJosh-PC.devlan.net.

Q. Do you see at the bottom there you circled the IP address?

A. Yes, I did.

Q. What is that?

A. This is the IP address of this computer. So if you saw activities that this computer was performing on the network, this is the IP address that would be shown, and you can know it belonged to this computer.

Q. What's the date of this file?
A. The date of this file is for April 12, 2016.
Q. Let's go to the next slide, please. This slide shows Government Exhibit 1209-2.
A. Yes.
Q. Where is this exhibit from?
A. This is from the ESXi server. This is another file that we recovered that portions of it were deleted.
Q. At the bottom it says "OSB ESXi server-unallocated space."
A. Yes.
Q. Does the server also have an unallocated space file?
A. Yes. It's not necessarily a file. It is just what we refer to as the space on a server that's either marked as free or currently not in use by any other files.
Q. You see at the top of the screen there is the IP address highlighted?
A. Yes.
Q. What is this exhibit showing?
A. This is just showing that there's a log-in through vSphere from the defendant's workstation on April 15.
Q. And a log into what?
A. To the ESXi server through vSphere.
Q. Let's go to the next slide. You also said that the defendant had a virtual machine on his DevLAN computer?
A. Yes.

Q. Is that referred to here as the Ubuntu X64?
A. Yes, it is.
Q. Is that virtual machine assigned a different IP address?
A. Yes, it is. It's configurable. You can have a virtual machine either use MAT, which lets it use the same IP as your host computer, or in this case you can have it set to a bridged mode where it can get its own IP address from the network. That's how it was configured in this case, and that's why the IP address is different.
Q. This slide has excerpts of 1203-19. Where are they from?
A. This is from unallocated space. These are remnants of what we call a lease. The Windows Active Directory server runs a service called DHCP, which is dynamic host configuration protocol. It essentially, when you plug a computer into a network, it has to get an IP address to talk to other computers on the network. And the server handles handing those out. These are the logs on the virtual machine that store information related to the IP address that that computer received.

We'll show a couple different ones just to cover a handful of days to show the IP address for this virtual machine remained 10.3.2.35.
Q. Just staying on the left photo that you just circled. What date does this reflect the IP address was 10.3.2.35?
A. This is, if we look down here at renew. I won't explain

all of these separately. But, if we look at the renew time, basically, when a computer gets an IP address, it doesn't just hold on to it forever. At least when it's configured to use DHCP. It is kind of required by standard to reach out and renew its IP address to the server so you don't end up with like 20 computers that have the same IP address and you have issues with your network. That's configured by a lease time. That's -- this is just seconds, I think it is 24 hours. And then it will automatically try to renew its IP address at this time, in this case 4:18.

So what this is just showing is that around 4/18/2016, the IP address for the virtual machine was 10.3.2.35. As we go through the next few slides, we see it was the same IP for a long time, so it just didn't change.

Q. Let's go to the next slide. Again, let's go on the right now.

So, what was the IP address as of April 19?

A. April 19 it was the same IP address. This 10.3.2.35.

Q. And the next slide. What was the IP address as of April 20?

A. The same IP, 10.3.2.35 and same for the 21st.

Q. We can go to the next slide.

MR. LAROCHE: This might be a good time to break.

THE COURT: We'll take our luncheon recess now. Resume at 1:30.

(Jury excused)

THE COURT: Ms. Shroff, do you want to take up your letter of Mr. Leedom?

MR. ZAS: I couldn't hear you.

THE COURT: I asked Ms. Shroff, did she want to take up her letter about Mr. Leedom.

MR. ZAS: I can handle it. As we said in the letter, our objection was to the inadequacy of the expert notice by the government. We got their expert notice in October of last year, October 18. And we quoted the portions in our letter, but there was no mention of an access to a March 3, 2016 backup file. And we think under the rules, the government should have at least supplemented, if they didn't know it then, they should have supplemented that information. So we're asking the Court to preclude that testimony as not adequately noticed.

THE COURT: Mr. Laroche.

MR. LAROCHE: Your Honor, just as an initial point, we think the notice was more than adequate, given we identified specific exhibits that Mr. Leedom relied on, which had that March 3 backup as part of the exhibit when we gave exhibits in August.

And to the notice point, defense counsel, after we gave the expert notice, actually asked for a copy of the backup itself, and we provided a copy of the March 3 backup itself to defense counsel and the defense expert in September, many

months ago. So the idea they didn't know that the March 3 backup would be at issue in this case is a little surprising.

And if they're focusing on a revised exhibit that the defense asked for that had the specific access time, as soon as we provided that to them, we provided notes from Mr. Leedom explaining his views of the document.

And, in advance of trial, we also gave them this presentation, weeks before trial, which detailed all the aspects of his testimony.

So they have been on notice for months, we believe, but certainly when they got the presentation and other materials in this case, and again, they asked for the actual backup that they're now saying they didn't know that we would be talking about. So, we think they're well on notice. And I also note that expert notice is not a script as to exactly what that person is going to say.

So, I think given the record here, it's pretty clear that they just don't want the testimony which is damning to Mr. Schulte to come in. But that's not a basis to exclude it.

THE COURT: I've considered the objection, I thank the government for its elaboration. I'm going to deny the motion. I don't think under Rule 16 you have to be as specific. I think the general notice that was given is more than adequate. Certainly the notice that was given as elaborated on by Mr. Laroche is more than adequate in the circumstances, so the

application is denied.

How much longer do you have?

MR. LAROCHE: I think he is going to take us through the end of the day, your Honor. I think probably two to three hours.

MS. SHROFF: I have one matter to raise with the Court.

THE COURT: Yes.

MS. SHROFF: Your Honor, from the beginning of this trial, I understand the Court has made some rulings on the protective measures. At the beginning of this trial we provided to the CISO in this case a list of attorneys that wanted to be present within the courtroom. This list included literally only people at the Federal Defenders office who do not have security clearance. For weeks we got no response. And today, after much follow up, we were told that the CISO would not authorize the lawyers to come in from our office or from the Federal Defenders office.

And then I got an e-mail from the Court's courtroom deputy informing me that he had spoken with the CISO, and that CISO's position was that no uncleared lawyer can be present in this courtroom.

We believe that deprives Mr. Schulte from a public trial, we believe that such a restriction is inappropriate, and I raise this on the record to object. Thank you, your Honor.

THE COURT: They can certainly attend the open sessions. They're free to attend in the overflow courtroom. But if you don't have a security clearance, as I understand what we've agreed to or what I've imposed in my order, is when the courtroom is closed, you have to have a security clearance in order to attend.

MS. SHROFF: Your Honor, there are reporters here. There are people with no security clearance here. And an attorney from the Federal Defenders office, I certainly do not see any risk of such a lawyer attending this courtroom proceeding.

THE COURT: I disagree with you, Ms. Shroff. I've made my ruling.

MS. SHROFF: Okay. One last thing that I just kind of remind the Court. Mr. Schulte has a continuing objection that we have laid out in writing to the video demonstration. I'm not sure Mr. Laroche intends to put that video in through this witness. But I just remind the Court that ruling is pending.

THE COURT: Thank you.

(Recess)

(Continued on next page)

AFTERNOON SESSION

1:30 p.m.

THE COURT: Please be seated.

Let's call in the jury.

(Jury present)

THE COURT: Please be seated.

All right. Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

Ms. Hurst, if we can just start with slide 36, please.

Q. Mr. Leedom, just before the break, we were talking about the IP address assigned to the defendant's virtual machine. Is that right?

A. That's correct.

Q. And on April 20 -- sorry. Let's start with April 19.

On April 19, what IP address was assigned to his virtual machine?

A. That would be 10.3.2.35.

Q. And that's 2016, is that right?

A. That's correct.

MR. LAROCHE: Let's go to the next slide, slide 37.

Q. On April 20, 2016, what IP address was assigned to his virtual machine?

A. The same IP address, the 10.3.2.35.

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

Q. I want to change gears a bit to certain events that

happened on DevLAN in April of 2016.

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

Q. Can you read this slide for the jury?

A. Yes. "April 4, 2016, the defendant loses privileges to Brutal Kangaroo and OSB libraries."

Q. And as part of your review of the materials in this case, did you see evidence of these things occurring on DevLAN?

A. Yes, I did.

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

Q. Can you read the title of this slide, please?

A. Yes, I can. "Changes to the defendant's project permissions." And then this is the name of a file, "Jeremy_abuse_of_power.pmg.

Q. And that's in quotes. Do you see that?

A. Yes.

Q. Why is that in quotes?

A. This is a name of a file that was found on the defendant's computer.

Q. What computer was it found on?

A. The defendant's DevLAN workstation.

Q. And where was it found on the defendant's workstation?

A. In his documents folder.

Q. Where is this exhibit from?

A. This is an exhibit showing the permissions for a project on Stash.

Q. How do you know it's Stash?
A. We can see up here, in the top left-hand corner, this Bitbucket, and then this is the Stash/Atlassian web -- website, as it were.
MR. LAROCHE: Let's just zoom in, if we can, on the left quarter of the screen where that picture is and Bitbucket. That's perfect.
Q. Can you circle Bitbucket.
What is Bitbucket?
A. Bitbucket is just another word for -- it's the Atlassian project that we've been calling Stash. It was renamed at some point.
Q. Is this a picture of Stash as it appeared on DevLAN?
A. Yes, it is.
Q. And what interface are we looking at to view Stash here?
A. This is through the web browser.
Q. What do you mean by through the web browser?
A. As you can see, like, at the top of the page, this is a common web browser, and you can see the address of the server. It's Stash.DevLAN.net.
MR. LAROCHE: If you could clear those for a second.
Q. Do you see on the right of Bitbucket there's projects, repositories, people and pull requests?
A. Yes.
Q. What's a project?

A. A project is essentially a source-code repository, so a -- it's a place where you would store source code.
Q. And what about a repository?
A. A repository would be, like, an individual, like -- it's the actual place that code goes. So you can have projects with different amounts of source code underneath them.
Q. And then you see there's a picture there of a kangaroo?
A. Yes.
Q. And below that it says Brutal Kangaroo?
A. Yes.
Q. What is Brutal Kangaroo?
A. It's the name of a project.
Q. And then to the right there, you see audit log in black?
A. Yes.
Q. What is this screenshot showing?
A. This is showing permissions, essentially a log file that shows permissions that have been added or removed or changed for this project.
MR. LAROCHE: Let's zoom out again, please.
Let's go to the next page.
Q. This is still Government Exhibit 1202-1. Is this a zoomed-in portion of that exhibit?
A. Yes, it is.
Q. Can you walk us through what this exhibit is showing?
A. This is just showing that on April 4, 2016, the following

permissions were changed for the project. We can see different permissions were modified, revoked and granted.

Q. And who made those changes?

A. These changes were all made by Jeremy Weber.

Q. And what changes were made to the defendant's privileges on Brutal Kangaroo?

A. They were removed.

Q. And did someone else get privileges that day?

A. Christopher was granted project admin access to the project.

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

Q. This is showing Government Exhibit 1207-53. Do you see that?

A. Yes.

Q. Where is this exhibit from?

A. This is from the NetApp server inside of a folder in Jeremy Weber's home directory, where they copied off some of the logs from Bitbucket.

Q. And Bitbucket is Stash, is that right?

A. That's correct.

MR. LAROCHE: Let's zoom in on this exhibit if we can.

Q. Can you walk us through, just starting at the top, what this is showing?

A. Yes, I can.

So, this first part here, this is the IP address of the

user that made the change. Overall, this, what we're looking at, is the server-side equivalent of the page on the previous slide, so these are just those -- this is just a log file for the changes that were made.

The IP 10.2.8.10 is Jeremy Weber's IP address, and as we saw in the previous slide, there's different types of events. For this first entry, this is a "project permission modification requested event," which just means that project permission has been requested to be changed.

This piece is the user that's requesting the change.

This is a time stamp.

In Linux machines and other servers, sometimes they'll store time stamp information in a number that looks like this. It's something called epoch time. It's essentially the number of seconds since January 1, 1970.

Q. Sorry. To pause you there, are you able to translate that time?

A. Yes, we can.

Q. And how do you go about doing that?

A. There's many different ways. I believe this is in milliseconds, so you can use any number of converters that can just convert this into the current time, and this is sometime on April 4.

Q. And next to that set of numbers is BK?

A. Yup. So --

Q. What does that refer to?

A. BK is -- this space in the log is saved for the project that's being modified, so BK is the product identifier for Brutal Kangaroo.

After this, we have this -- let me just clear this really quick. We have the specific permission that's being changed and the user who is being affected by that change.

These last two fields, at the end, here to here, have to do with, like, session ID information for the server and the user session that made the change. They're not explicitly important for this exhibit.

You can see the way these are organized, we first have -- like, we have two events that are kind of paired together. The first is a modification request, and then there's the actual modification event. So we had a request to change "project write" for user Schuljo and the old permission and "project admin" to "new permission project write."

And then if you read through the rest of this, we can see that, as it kind of bubbles down, at the end we have "project permission revoked event" for Schuljo, meaning his access to the project was removed.

Q. And then it's, I guess, the last four lines there, what events did those reflect?

A. This is a permission grant for the Christopher user as project admin for the Brutal Kangaroo project.

Q. Who conducted these activities on the system?
A. Jeremy Weber.
Q. And are these the same activities that were reflected on the previous slide?
A. Yes, they were.
MR. LAROCHE: Let's go to the next slide, please.
Q. This is showing Government Exhibit 1207-53. What is this exhibit from?
A. This is from the same location, on the NetApp in Jeremy Weber's home folder in the Bitbucket logs that they saved off.
MR. LAROCHE: And if we can zoom in on this exhibit again.
Q. Let's just focus on the first four lines or so.
A. Yes.
Q. What do those logs reflect?
A. These are more permission revocations for the defendant by Jeremy Weber, this time for the OSB libraries project.
MR. LAROCHE: OK. We can zoom out.
Let's go to the next page, please.
Q. As part of your review of materials in this case, did you identify certain activities of the defendant on DevLAN on April 15, 2016?
A. Yes, I did.
Q. What were some of those activities?
A. One of them was that he attempted to mount the Altabackups

to a different location. He tried to create a data storage for the Altabackups on the ESXi server, and then the second was that he logged in with an administrative session over SSH to the ESXi server, using his public-private key pair.

Q. Just on the second bullet for a moment, what type of administrative session are you referring to there?

A. This is a server administrative session for the server administrator.

Q. For what server?

A. For the ESXi server.

Q. And how did he log in to that administrative session?

A. Using SSH, through his Ubuntu virtual machine on his DevLAN workstation.

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

Q. This is showing Government Exhibit 1209-9. Do you see that?

A. Yes.

Q. Where is this exhibit from?

A. This is a log file from the ESXi server called host D.

Q. Let's just focus on host D for a moment.

A. Yes.

Q. What's the host D log file?

A. The host D log file contains information primarily related to VMware vSphere and vCenter. Specifically, we'll see it in this presentation where it shows log-in events from those

services.

MR. LAROCHE: Let's zoom in on this log file for a moment.

Q. Why don't we start on the top two lines and just the top left.

A. Yes.

Q. Just walk us through, first, the date and time of this log file.

A. Sure. So, this is from 4/15, 2016, at 7:36:05 UTC, and we're looking at a log-in -- let me clear this really quick -- from a DevLAN user, the defendant, from this IP address. And this is just showing that he's logging in using vSphere.

Q. The first thing you said on the time was a reference to UTC?

A. Correct.

Q. What's UTC?

A. UTC is the same as GMT or Greenwich Mean Time. It's the time zone, like, all other time zones are based off of. So if we were to convert this into local time, we would subtract four hours from it, so 7:36 would be 3:36.

Q. Do you see the user DevLAN/Schuljo?

A. Yes.

Q. What is that?

A. So, when you have an account on Active Directory, you'll have a username and then the domain to which that username

belongs. In this case the domain was DevLAN and the username was Schuljo.

Q. And what is he logging into here?

A. He's logging into the ESXi server through vSphere. This would allow you to connect to different virtual machines and manage those services.

If we look at the second line, this ticket issued for MKS service to user. MKS stands for mouse, keyboard, screen. So if you remember earlier, when I spoke about you could go into vSphere and click on the virtual machine and get, like, a shell session for it and then you would be presented with the actual operating system of the virtual machine, this is saying that action happened.

Q. Is this a log-in as a regular user or as an administrator?

A. This is a log-in as a regular user.

Q. How, if at all, would this file look different had the defendant logged in as an administrator?

A. If it was an administrator user, you would see this "user equals" and this user here at IP address. Instead of the username being DevLAN Schuljo, for example, you'd see the word "root."

Q. What does root refer to?

A. Root is the administrative user in a Linux computer.

MR. LAROCHE: Let's zoom out again, please.

Q. This activity, this log-in, occurred at approximately what

time?

A. 3:36 p.m.

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

Q. This slide is Government Exhibit 1202-7. Where is this exhibit from?

A. This exhibit's from the defendant's DevLAN workstation, specifically a log file for the vSphere client software.

Q. At the bottom it says VI client?

A. Yes.

Q. What does that refer to?

A. So, the VI client is, and we'll see it in logs here, like where it says VI client, these are logs that are generated when you use the vSphere application.

Q. The last slide was a server-side log, is that right?

A. That's correct.

Q. Where is this log from?

A. This log is from the defendant's workstation, otherwise known as the client. So, when you have a server and you have connections between that server and another computer, one will be the client and one will be the server. In this case, this is from the client, or the defendant's workstation.

It's important to note the difference, because there's multiple exhibits from each. And when we see time stamps on the client's side, here, they are in EST, Eastern Standard Time, but the time stamps that we see on the server are in UTC.

Q. Why is that?
A. The server was just configured to operate that way.
Q. So let's take a look at the first two lines of this slide.
MR. LAROCHE: If we can zoom in on that, please.
Q. What are these two lines showing?
A. This is showing the defendant trying to create a NAS data store on the ESXi server that could be used with other virtual machines.
Q. Let's start first with what is a NAS data store?
A. So, I'll first explain what a data store is on ESXi.
A data store is simply a place where, a location where you can store data, and what you could do in this case with a NAS data store, which stands for network attached storage, is you can create this object. In this case, we'll see that it was to point to the Altabackup, and then you could attach that as a virtual hard drive to other virtual machines to access that data.
Q. What time did these activities take place?
A. At 3:47 p.m. on April 15.
Q. And where did he attempt to create the data store?
A. On the ESXi server.
Q. How do you know that?
A. We know it because that's how you create data stores, and since this is a VI client log through vSphere and he's logged in to vSphere through the ESXi server, that's where it's being

created.

MR. LAROCHE: Let's zoom out again, please, and if we could zoom in on just the rest of the exhibit, please.

Q. What is this showing?

A. This is the configuration information for the data store that the defendant was trying to create. This has things like the IP address of the server, the name of the share and what they were going to call the name of the data store itself, in this case backup, and the access permission, so --

Q. What does a data store allow you to do?

A. It essentially allows you to access the content. So, in this case, it would allow you to access the content of Altabackup through a data store called backup.

MR. LAROCHE: Let's zoom out again.

Let's go to the next slide.

Q. Did the defendant successfully create this data store?

A. No, he did not.

Q. Showing you a slide with Government Exhibit 1202-8, what is this exhibit from?

A. This is a continuation of the log in the previous slide, which came from the defendant's DevLAN workstation from the VI client log.

Q. And where is the IP address for the defendant's computer on this slide?

A. It's not on this slide.

Q. Then how do you know the defendant conducted these activities?

A. Because it's from the event we saw in the previous slide, and your client log on your machine is only going to show logs of activities from things that happened on your machine.

MR. LAROCHE: Let's zoom in on the highlighted portions of this slide, please.

Q. What is this showing?

A. This is showing that the attempt to create the data store ultimately failed.

Q. Why did it fail?

A. From this we can't tell why it failed other than that we got a permission-denied error from the NFS protocol, from the NetApp server.

Q. Are you familiar with the term "white list"?

A. Yes, I am.

Q. What does that refer to?

A. A white list is where you keep a list of machine names or IP addresses that are allowed to explicitly access a service.

Q. If the IP address for the server was not on the white list, would the permission fail here?

A. Yes, that could be a reason why it failed.

Q. Why is that?

A. Because only services that were maintained in this white list would be allowed to access that share.

MR. LAROCHE: If we could go to the next slide, please.

Q. Now, earlier you talked about the mount points for the Atlassian products?

A. Yes.

Q. Can you just draw a line from the Atlassian products to the Altabackup to show where those mount points were located?

A. Yes, I can.

So, Confluence had one. Bamboo had one. Stash had one. Crowd -- this -- let me undo this.

Since these were a, these weren't virtualized services in Stash and Crowd, so this mount point was actually up here from the Stash server. And then from Hickok to Jira as well.

Q. The last two slides we saw a data store that was attempted to be created on a server?

A. Yes.

Q. Can you show us what connection that would have provided to the backups?

A. Yes. I'm going to clear this.

This would have gone from the ESXi server itself to the backup.

Q. And had that been successful, how would you have accessed that data store?

A. You would have added it. You could have added it to any of the virtual machines on the ESXi server as essentially what

would be an additional hard drive.

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

Q. This contains Government Exhibit 1209-13. Where is this exhibit from?

A. This is a log file from the ESXi server.

Q. Where on the ESXi server was this log file found?

A. On the physical machine in the server log folder.

Q. Is there a particular log that this shows?

A. Yes. This is what we call the auth.log.

Q. What's the auth.log?

A. Auth.log shows connection attempts and other information, such as if a password's changed for the server, so what users or IPs were connecting to the server, whether they were authenticating with username or password or the SSH protocol.

MR. LAROCHE: Let's zoom in on this exhibit, please.

Q. Do you see on the left the third line down starts 2016-4-15?

A. Yes.

Q. Let's start there. What is that line showing?

A. So, this line, and I'll kind of circle it a little bit here.

This line is showing a connection attempt that is starting from the IP address 10.3.2.35, in an attempt to authenticate to the server.

Q. Whose IP address is that?

A. This is the IP address for the defendant's Ubuntu virtual machine on his DevLAN workstation.
Q. What time did this connection attempt to take place?
A. This connection was initiated on April 15, 2016, at 7:38 UTC, so 3:38 p.m.
Q. Let's go down to the next line, please.
A. This says that the server was unaware of the current host name that the IP address had. The last time it had seen it, it was called ndb-testrange-4.devlan.net. It's a security feature for SSH and authentication modules just to prevent something called a man-in-the-middle attack. This is -- yeah, it's not that important for this. It's, it's -- it was just a -- the server hadn't seen a connection from this IP address with a host name it recognized.
Q. What's the next line down that starts "accepted public key"?
A. This is saying -- over here on the left a little farther, we can see the protocol that's being used to authenticate to the server. SSH, as we talked about, is secure shell. This is saying that it was being used with a public-private key pair from this IP address; it's the same as above. And for that public-private key pair, this is the key fingerprint.
Now, a key fingerprint is a way to identify -- it's a unique identifier for a specific public-private key pair, and we know this to be the defendant's public-private key that's on

his Ubuntu virtual machine.
Q. How do you know that?
A. I've calculated the fingerprint and compared it, and it matches.
Q. Let's go down to the next line, please. What's that line show?
A. This is saying that the session was successfully authenticated, and it was opened for the root user.
Q. Do you see on the right there is a UID equals zero?
A. Yes.
Q. What does that mean?
A. That's saying the, like, system service authenticated it successfully.
Q. And then you do you see how the last few lines on the left there was a number in parentheses?
A. Yes.
Q. And it ends in 763?
A. Yes.
Q. Let's go down one more line. That starts 766?
A. Yes.
Q. Do you see that?
A. I do. I'll circle it here.
Q. What is that number?
A. This is an important number. When you log in to an ESXi server, your session is tagged with a certain ID. VMware calls

this a work ID, and anything you do while you're in that session --typing on the command line, things like that -- it's logged with this identification number, and it's meant to take back to this specific file to see who had logged in.

Q. Does that number now relate to the defendant's IP address in any way?

A. Yes, it does.

Q. How does it relate to his IP address?

A. Since this is the work ID for this session that we've been analyzing, we know that the activity that we see from this session, which this identifier number is unique and is never reused, came from 10.3.2.35.

Q. So on the line next to 766, can you explain what the rest of that line means?

A. Yes, we can.

It says "session opened for 'root' on /dev/char/pty/t0." This just means that it gave the requesting client, the defendant's Ubuntu machine, a terminal session to the server.

Q. What do you mean by terminal session to the server?

A. Terminal session, so the T0 -- or the PTY. I believe it stands for pseudo Teletype. It's in relation to old terminal machines that you would use where it was just a keyboard and a terminal window. These are since virtualized now in modern computing. So T0 essentially means that that's, like, the first available session. So if you were the only user to log

in to a server, in most cases you would be assigned to terminal zero. That's just showing what's been assigned here.

Q. Did this session -- the defendant's session, logged in as 766 -- ever close?

A. No. There's no evidence of this session ever closing in the log file.

If I erase here for a second, there's a separate section, lower on here. I won't go through every piece, but we can see that it was opened here. And then when that session ends, we'll see a pair for session closed and then another session closed for that user.

Q. And just to focus on that other session, when was that one opened?

A. This is the session that was opened on 4/16, 2016, when Jeremy Weber, which we know from this IP address, 10.2.8.10, logged in to the ESXi server and changed the root password. He then logged out on the 18th, in the morning, which I believe was the Monday afterwards.

Q. Do you see on the line where it says "session opened for root" there's a T1 at the end?

A. Yes.

Q. Why is there a T1?

A. There's a T1 because the T0 was already occupied by the defendant's session. So essentially, the defendant logged in on 4/15, and the session was open until the server was

repurposed on April 25, when they migrated the services over to ISB.

Q. And do you see at the bottom there, second-to-last line, it says "session closed for root"?

A. Yes.

Q. And that's for the T1?

A. Uh-huh.

Q. Do you see a similar session closed for T0?

A. No. There isn't one.

MR. LAROCHE: Let's zoom out for a second.

Q. When did the defendant log in as an administrator to the ESXi server on April 15?

A. At 3:39 p.m.

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

Q. Showing you Government Exhibit 1203-18, what is this exhibit from?

A. This is something we recovered from the defendant's Ubuntu virtual machine on his DevLAN workstation from an allocated space.

MR. LAROCHE: If we can zoom in on the highlighted portion, please.

Q. Let's just start at the top, root@OSB. What is that?

A. Part of what we were able to recover from the defendant's virtual machine was the actual text input and output from his session with the ESXi server that we just spoke about. This

part -- we can't date these commands specifically. We just know that they were run at some point after April 15, when he logged in to the server. The first command he runs, as we've discussed before, this root@OSB is just the username at what server, so we know he's logged in as root on the ESXi server.

The little tilde shows he's in the home directory for the root user. And this command, last, is a typical Linux command that's available on most Linux operating systems. What it does is it shows you the last successful log-ins to -- to the machine.

Unfortunately, Linux is an open-source operating system and can be customized by companies in different ways and support different software. In this case, the "last" command is not available in the -- as a command on this ESXi server, so a similar command to last that is available is the command "who." And who just shows who is currently logged on to the server. And in this case, it shows the root log-in from April 15 on T0 from the IP10.3.2.35, which is the defendant's DevLAN workstation virtual machine.

Q. And just at a very basic level, what does it mean to run a command?

A. So, running a command just means you typed it out on your keyboard and hit enter, and then the command text would be displayed to you on the screen for the output of the command.

Q. What was the output of this "who" command?

A. It was this line where you see here where I circled stuff: this root, the terminal, and the other information.

Q. And what does that output reflect?

A. This output shows that there's a user logged in to the ESXi server as root, with this terminal identifier, with this IP address, and the session was initiated at this time.

MR. LAROCHE: We can go to the next slide, please.

Q. This slide is titled "April 16, 2016," so I want to turn to that day. Did you see evidence of any activities occurring on DevLAN that day?

A. Yes.

Q. What did you see?

A. On April 16, passwords were changed and updated on the Atlassian products and the ESXi server.

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

Q. Now, this contains Government Exhibit 1209-16. Where is this exhibit from?

A. This exhibit comes from the ESXi server itself in the file that stores public keys for SSH to be used with authenticating to the server. Now, unlike the authorized-keys file from the Confluence server that had six or so different public keys available to use to log in, the ESXi server only had one key, which was the defendant's public key.

Q. Can you circle on the bottom right-hand corner of this exhibit schuljo@devlan.net?

A. Yes, I can.
Q. What does this mean?
A. This is the username of the user who created this key, the key pair, when it was created.
Q. And there are an awful lot of numbers and letters here. What are those?
A. This is a representation of what's essentially just a large number. This is a public key, which I discussed slightly earlier. It's mathematically related to the private key and can be used to verify itself that way.
Q. And where was this public key located?
A. This public key was located on the ESXi server in the authorized-keys file.
MR. LAROCHE: OK. Let's, if we can, go to slide 17.
Q. Just circle where this key was located.
A. This key was located on the actual server itself.
Q. And is this public key what was used to log in to an administrative session on April 15 --
A. Yes, it was.
Q. -- 2016?
Now, were there other keys located on Confluence?
A. Yes, there were.
Q. And just circle where they would have been located.
A. Those keys would be on the Confluence virtual machine running on top of the ESXi server.

MR. LAROCHE: Let's go to slide 53 for a moment.

Q. This has exhibit 1203-9. Where is this exhibit from?

A. This is from the defendant's DevLAN workstation in his Ubuntu virtual machine.

Q. What is it?

A. This is the private key, which is the pair to that public key that we were just looking at.

Q. What do you mean by a pair?

A. Like I'd mentioned before, a public-private key pair, they're mathematically related so they can be used to log in through the SSH protocol. It's something called asymmetric cryptography.

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

Q. Was the defendant's private key encrypted in any way?

A. Yes, it was. Actually -- so, this is the password for the key.

Can we go back a slide?

Q. Sure.

A. And if you look at the top of the private key, you can see whether the key's encrypted or not, and this shows us that it was encrypted.

We can continue back to 54.

This was the password used to decrypt that key. What this means is if you create a private key with a password, not only do you have to have the private key to log in, but you have --

it will prompt you for a password when you try to use it, and if you don't know that password, you can't log in with it.

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

Q. Showing you Government Exhibit 1207-2. Where is this from?

A. This is from the NetApp server in the defendant's home folder.

Q. What is this exhibit showing?

A. This is a private key and public key that the defendant had for another user on DevLAN called -- his name was Rufus.

Q. Where did Rufus work at the CIA?

A. I don't -- I don't recall. It was somewhere in EDG. I don't remember which specific branch.

MR. LAROCHE: Could we go to the next slide, please.

Q. What's this showing?

A. This is the, just the public key for Rufus's key, also on the NetApp in the defendant's home folder.

Q. Where was this found?

A. On the NetApp server in the defendant's home directory.

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

Q. This slide has Government Exhibit 1207-92. Where is this exhibit from?

A. This is from the Confluence backup, the whole virtual machine backup, that was stored on the NetApp server when they did the migration.

MR. LAROCHE: If we could zoom in on the exhibit and

the black boxes to the right.

Q. What is this exhibit showing?

A. This is a configuration file for the Confluence virtual machine. This shows the snapshots that were available for that machine. We can see that there were three snapshots, snapshot 1, snapshot 2 and snapshot 4, and this is as of April 25, when they migrated the service and made the backup copy. These are dated using this "create time" high-low value. This is just a machine-stored version of this. If -- you can go online and look up how to convert this, and there's a Python script available online, and you just essentially have to subtract these two numbers and you can get the human-readable time stamp.

The first snapshot is the snapshot that was created when the Confluence instance was installed. I'm going to clear this real quick. Confluence installed.

The second snapshot was when the backup was made before they changed the passwords on April 16. And that that time stamp is again reflected over here from April 16 at 1:42.

And then this snapshot 4 -- you'll notice we go from snapshot 2 to snapshot 4. There's no snapshot 3 here because that was a snapshot that the defendant had created and then subsequently deleted. But VMware keeps track of how many snapshots it's made in the past, so when they made the snapshot to back up before the network changed, it was given the number

4, and that was on April 25.

Q. Let's just circle snapshot 1 on this screen.

Snapshot 2.

And snapshot 4.

You said that snapshot 3 does not exist because it was deleted?

A. That's correct.

Q. By whom?

A. By the defendant.

Q. Why is there a snapshot 4 if no snapshot 3 appears here?

A. VMware keeps track so it knows when the next snapshot was made that it needs to be indexed as No. 4. It's to show things just as this so you can know how many times the machine's been snapshot -- snapshotted in the past.

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

Q. This is showing Government Exhibit 1207-7. Where is this exhibit from?

A. This is from the April 16 Confluence snapshot in the SSH authorized-keys folder.

Q. And what do each of these blocks of text reflect?

A. These are public keys from SSH public-private key pairs for all of the different keys that were available to log in to Confluence as of 4/16, before they changed the passwords.

Q. And where were these keys located?

A. There's a file in the SSH folder on Linux system that

stores what public keys are available. It's called authorized keys.

MR. LAROCHE: If we can just flip back quickly to slide 17.

Q. Just circle where these keys would have been located.

A. So, these keys were on the Confluence VM.

Q. This is different from the key we viewed earlier that was the defendant's public-private key on the server, is that correct?

A. That's correct.

MR. LAROCHE: We can go back to Government Exhibit 58.

Now, let's zoom in on the second-to-last key.

Q. What is this key?

A. This is another public key. It's labeled as root@jira.ioc.local. This key was likely generated on the Jira Confluence application.

Q. And what significance, if any, is there to the fact that it's on the Confluence virtual machine?

A. If you zoom out again, we can see another, similar key to this both from dev-01 and from Bamboo. At some point, either when the Atlassian services were set up or shortly after, it appears that a public-private key pair was made for each of the services and used in some way. We can't say for certain exactly how this was used, but you would need the private key that was associated with each of these public keys to log in

this way.
Q. And if you had that private key, how could you log in to the Confluence virtual machine?
A. By using SSH.
Q. And would you have administrative access at that point?
A. Yes, you would.
Q. So if the defendant used his private key on April 16, 2016, while this key was still there, would he have had administrative access to the Confluence virtual machine?
A. Yes, he would, and the defendant's private key -- public key is also here, up at the top.
Q. You talked about mount points earlier to the Altabackups?
A. Yes.
Q. Where was the mount point for Confluence located?
A. In the slash mount Altabackup folder on the Confluence server, virtual machine.
Q. If you used the SSH key shown on this slide to log in to the virtual machine, would you have had access to those mount points?
A. Yes, you would have.
MR. LAROCHE: Let's go to the next slide, please.
Q. This is showing Government Exhibit 1207-18. Where is this from?
A. This is from the April 25 Confluence snapshot. So, forensically speaking, we got to the network obviously after

this machine had been migrated, so our image of the Confluence server came from that backup that they made when they transitioned the Confluence and Bamboo machines to ISB on April 25. So our most recent copy of that service was from here, and this just shows us the authorized-keys file after the passwords were changed on the 16th.

Q. Is this the only authorized key in that folder after April 16, 2016?

A. Yes are. They deleted the rest of them -- well, they deleted all of them and added this new key which was created.

Q. Is the defendant's key available in this authorized-keys folder after April 16, 2016?

A. No, it's not.

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

Q. This contains Government Exhibits 1207-10 and-11. What are these exhibits from?

A. These exhibits are from the Confluence virtual machine from the April 16 snapshot before they changed the passwords.

Q. And generally, what are these files?

A. There's two files that are represented here. On a Linux machine, the way user accounts and their passwords are related are they're stored in two files. One's called the password file, which we have here on the left. The second is called the shadow file, which we have on the right.

The password file stores user account names, what groups

they're in, things like what default shell they have. And the file on the right stores the password for those users.

You'll notice that on the right here, there's only two accounts that have this big, like, long string of numbers in it. This is a hash of that password.

The other accounts that are listed here, you'll see they have a little asterisk. This just means that account was never assigned a password and can't be used to log in.

(Continued on next page)

Q. What is this password for?
A. So, this password is for the actual root user account. If you were to log in through vSphere into the ESXi server, click on the Confluence virtual machine, and then click the little box that gave you a shell session into the Confluence VM, and it would prompt you for a user name and a password. And you would give it root, and the password, this is a hash of the password. A hash is simply a function to obfuscate the password, because you wouldn't store the plain text password in a file. If someone got on the system they could see it and reuse it.

So, this slide is just to demonstrate, as we'll see I believe on the next slide, that this password was changed.
Q. Let's go to the next slide, please. These are similar exhibits; is that right?
A. That's correct.
Q. Do those exhibits reflect a password change?
A. Yes, they do.
Q. How do you know that?
A. So, this is from the April 25 snapshot of the Confluence VM. And if you compare this long hash for the root account on this slide to the last slide, you'll see that it was changed, indicating the password was changed.
Q. So we've been talking so far about changes to the Confluence virtual machine. Is that right?

A. That's correct.
Q. So what changes have we seen so far to the administrative privileges on the Confluence virtual machine?
A. We've seen that all of the public keys that were on the machine were all deleted and a new one was placed in. And then the administrator account, the actual user account on the machine had its password changed as well.
Q. So let's now switch gears to the OSB ESXi server itself. Go to the next slide, please.
Were there any changes to that server on April 16, 2016?
A. Yes, there was.
Q. So we saw this slide, this exhibit several slides ago. Is that right?
A. That's correct.
Q. You said that this is the auth. log from the ESXi server?
A. Yes.
MR. LAROCHE: If we can zoom in on the activity from April 16, 2016, please.
Q. What is this showing?
A. This is showing the activity that Jeremy performed when he logged into the ESXi server, and then changed the password for the root account.
Q. Can you circle how you know that he changed the root account.

A. Yes. At the very last line here, we see password changed for root.

Q. Again, how do you know this is activity that was done by Jeremy?

A. We have his IP address which is 10.2.8.10.

Q. Were you able to confirm that password change?

A. Yes, we were.

MR. LAROCHE: So let's zoom out for a moment and go to slide 63, please.

Q. Showing you Government Exhibit 1209-15, the top half of this slide. Is that the exhibit?

A. Yes, it is.

Q. Let's zoom in on that for a moment. What type of file is this?

A. This is a shadow file. We reviewed one similarly for Confluence a few slides ago. This has the pass -- the hashed password for the accounts on the system.

Q. What is this file from?

A. This is from the ESXi server.

Q. Let's zoom out. What's the bottom half of this screen showing?

A. I manually calculated the password for this hash, just to show that the hash was changed and that, in fact, it was changed from the password My Sweet Summer which existed on the server prior to 4/16/2016 to a new password that we'll see

after 4/16. We can do this by -- the way these hashes are calculated, it essentially takes your password, and then it takes a random bit of data which is called a salt and it adds that to your password to make it unique. And then it hashes it with a common hashing algorithm. This $6 specifies exactly which algorithm was used in this case, I believe 6 is SHA-512. It is just a mathematical function that generates this string of numbers you see here.

You can use a standard library in python which is a scripting language to verify that plain text password matches a hash. So we're just doing that here.

Q. What is the password on this screen?

A. This password is My Sweet Summer.

Q. Could you verify that that changed?

A. Yes, you could, if you compared it to the new version.

Q. Were you able to do that?

A. Yes, I did.

Q. Let's go to the next slide, please. What is this slide showing?

A. This is showing the shadow file after the password was changed. We can see here that the new hash matches.

Q. Go to the next slide, please. Sorry, just one slide back. I don't think I asked.

What was the new password?

A. The new password is up here a little more easy to read.

I've been saying it as "To Make a Call" with some symbols in it.

Q. Let's go to the next slide, please. Showing Government Exhibit 1209-16.

Did we see this before?

A. Yes, we did.

Q. What is this?

A. This is the defendant's public key that is on the ESXi server.

Q. Did this key remain on the ESXi server after April 16, 2016?

A. Yes, it did.

Q. Do you see evidence of the defendant using his administrative access to that server after April 16, 2016?

A. Yes, we do.

Q. We'll come back to that later. If we can go to the next slide, please.

This is titled "Recap, April 16, 2016." What is this slide meant to convey?

A. This is just showing the changes that were made to the network, specifically to Confluence and the ESXi server when they changed the passwords.

Q. What changes were made to the server itself?

A. The ESXi server itself?

Q. Yes.

A. The administrative root password was changed, but the SSH key for the defendant was not removed.

Q. Go to the next slide, please. So I'd like to turn your attention to April 18, 2016. Do you know what day of the week that was?

A. I believe it was a Monday.

Q. Let's go to the next slide, please. This is showing Government Exhibit 1095, a memorandum to Joshua Schulte from Anthony Leonis dated Monday, 18 April 2016.

If we could go to the next slide, please.

Mr. Leedom, can you please read the text that's excerpted here on this slide?

A. Yes, I can.

MS. SHROFF: Objection, your Honor. This is far beyond the scope of an expert's testimony. This slide has nothing do with his expertise.

THE COURT: Okay. The objection is overruled.

MR. LAROCHE: Thank you, your Honor.

Q. Please read it, Mr. Leedom.

A. Yes. "Lastly, effective 0800 on Monday 18 April, the OSB libraries (and any associated computer network exploitation CNE related code libraries, development tools, etc.) will be administered by a designated AED/OSB personnel until further notice. Please do not attempt to restore or provide yourself administrative rights to any project and/or system for which

they have been removed. The undersigned has read and understands the above." And we have the defendant's signature.

Q. Let's go to the next slide, please. Showing you Government Exhibit 1063 which is an e-mail sent on April 18, 2016, at 12:59 p.m. from Joshua Schulte to Anthony Leonis, and the subject is "ISB infrastructure permissions transfer."

Can you remind us what is ISB?

MS. SHROFF: I have the same objection.

THE COURT: Same ruling.

A. ISB is the infrastructure support branch, that, from what I understand, managed some of the services that were in place for EDG.

Q. Let's go to the next slide, please. Can you please read the excerpt that's on the screen.

A. The entire excerpt or just the first part?

Q. Let's start with the top sentence.

A. Okay. "I verified that all private keys with access have been destroyed/revoked."

Q. And then, in the second paragraph, start with "it seemed."

A. "It seemed like overnight literally all my permissions within the products were removed and all my permissions on servers themselves revoked ... and all without anyone informing me. Is there a reason to this sudden turnover that occurred without my knowledge?"

Q. Have you reviewed forensic activity on the network from

April 18, 2016?
A. Yes, I have.
Q. Did that include reviewing log files from the defendant's DevLAN computer?
A. Yes, it did.
Q. What are some of the defendant's activities on the DevLAN network on April 18, 2016?
A. We see him logging in to vSphere as the root administrator user as well as utilizing his session on the ESXi server which was initiated on April 15.
Q. Was the defendant's private key to the ESXi server destroyed or revoked?
A. No, it was not.
Q. How do you know that?
A. We know that because it was used to authenticate with the session on the server.
Q. Were all of the defendant's permissions on the servers themselves revoked?
A. No, not all the servers.
Q. Which servers were they not revoked on?
A. The ESXi server.
Q. How do you know that?
A. His public key was still in the authorized keys file on the ESXi server, which would allow him to have accesses to that server.

Q. Did you see the defendant log in as the administrator to the ESXi server after April 16, 2016?
A. Yes, through vSphere.
Q. What does that mean?
A. That means he utilized the root account and password for vSphere to log in that way.
Q. So let's go through some of the activities on April 18, 2016. If we can go to the next slide, please. I'm showing you Government Exhibit 1203-16.

Where is this exhibit from?

A. This exhibit comes from the defendant's DevLAN workstation in his virtual machine recovered from unallocated space.

MR. LAROCHE: If we can zoom in on the top third of the highlighted text, please. Let's start at the top line.

Q. What does root@Josh-desktop mean?
A. Josh-desktop was the host name for his Ubuntu virtual machine on his DevLAN work station. And root was the account he was logged in at the time these commands were run.
Q. What's the next set of commands on that line?
A. This is showing the folder that he was in, the dot SSH folder, and he did a list command to show the files in that folder.
Q. What's dot SSH refer to?
A. A dot in a folder in Linux means it is a hidden folder. This folder is hidden by default, because it typically stores

private keys for users, and it's a simple but -- it is simple, but it is a security mechanism for that.

Q. Below that there is a total 20?

A. Yes.

Q. What does that mean?

A. When you run the LS command and give it the -- the L flag, I'll just explain both the flags.

A flag is like an argument for a command. So this just says run the list command and give me some extra information. In this case, the A says list all files, including hidden files. And the L says give me file details. When you run the command this way, you can get a total, and the total is the number of 512 byte blocks that are occupied at the physical file system level by the files in this folder.

So, it is essentially just a quick way to sum up the size of the files in that folder.

Q. Then, below "total" there is a DRWX. Do you see that?

A. Yes.

Q. What is that?

A. So, these are permissions for individual files and folders in this directory. It's split up into three parts here. I'll try and circle it. It's going to be a little difficult.

So, this first is a special bit. In this case a D stands for directory. In Linux, you have folders, and obviously at the command line level, you have to type to move

between different folders. So, if you see to the far right, there is a little dot here. That's just the way that the Linux shows you that's the current folder that you're in. So if you wanted to run a command, or like, let's say you had a script or a file in that folder you wanted to run, you would append it with a dot forward slash, meaning the folder I'm in accessed this file. Something like that.

Right below, we have a dot dot. This represents the folder directly above this one. So if you wanted to change directories to the folder that is above you, you would use the CD command, which is the change directory command. And then give it the dot dot, which would move you up a directory. We'll see some examples of those other commands later on.

But, this D bit here just indicates that this is a folder. You'll notice there are the files over here on the right, ID_RSA and known_hosts, these are just text files. These don't have the D in the front.

The rest of this set of dashed lines, these are sets of permissions for different things. The first one is the permissions for the owner of the file, the second is the permissions for the group that the owner is in of the file, or the group that the file is assigned to, excuse me. And then the last set of three things here is the permissions for anyone on the system for the file.

So if we put it together for this ID_RSA file, this is

saying that the root user has read write access. This last bit is the execute, which means it allows that file to be run as a program. That's not on this particular file, that's why we have a dash.

The group that that user is in, it's a little confusing since the root user is in the group that's called root, which is like the administrative group. That group just has read access.

And then if you happen to log in and you're not the root user, you fall into this everyone category, and you would only have read access to this file.

Q. So let's go down a couple lines to root@Josh-desktop, then there is SSH SSH root@Stash, do you see that?

A. Yes.

Q. What is that showing?

A. This is how you would instantiate the SSH command if you are on the terminal and you wanted to log into the server. In this case we're asking to log in as the root user to the server called Stash.

Q. Can you tell from this log file whether this log-in was successful?

A. No, we can't. Not from what we have here.

Q. So let's zoom out. Then zoom back in on the middle portion of this log file. Generally, what is this showing?

A. This is another -- well, at the top we have a list command

showing the files in this folder again. This time it's just formatted a little bit differently because it wasn't given those AL flags. And below this we have another SSH command to log in as the root user to the Confluence server.

Q. When you refer to the Confluence server, are you referring to the virtual machine?

A. Yes, I am.

Q. To be clear, were the defendant's SSH keys for the virtual machine revoked?

A. Yes, they were.

Q. Can you tell from this log file whether this log-in was successful?

A. No, we cannot.

Q. So let's go to the last bit of text that's highlighted at the bottom. What is this showing?

A. This is showing a log-in to the Jira server. The first two lines here, the defendant attempted to use the host name for Jira which was the human readable name which is Jira.IOC.local. And his virtual machine didn't know how to resolve that. So, the fallback is you have to manually enter the IP address for the server, which is what he did here. This is just connection information to the server. And then the server requests a password to access. And we see that the permission is denied after three failed password attempts, and he was unable to log into the Jira server.

Q. Let's go to the next slide. Showing you Government Exhibit 1207-26. Where is this exhibit from?

A. This is from the Confluence virtual machine in the auth. log file.

Q. What is this showing?

A. This is showing when the defendant's virtual machine at 10.3.2.35 attempted to log in over SSH to the Confluence server on April 18, at 11:08 a.m.

Q. Why did that fail?

A. It failed because his public key was no longer on the server. So he was unable to authenticate to the server.

Q. Was there another attempt attempted log-in at 11:13 a.m.?

A. There was.

Q. Can you explain what happened there?

A. We can see by the information in the log file that this wasn't an SSH log-in, this was like a normal log-in. And we can tell that from, when we see mention of the pam_unix module, this is what handles authenticating user names and passwords on a Linux system. And this is when someone tried to log in using vSphere in the shell session, and was prompted with a password user name and typed it in, and then in this case we have a failed log on.

Q. So let's talk about the vSphere log on for a moment.

A. Yes.

Q. Please explain how the defendant would use vSphere to log

in.

A. So you double click the application and it asks you for credentials to log into the ESXi server. Typically you would use your DevLAN user name and password, and it would let you in. And then you'll be displayed with a list of all of the virtual machines that are on the server, and you can select one, in this case, the Confluence virtual machine. And you would click on a little shell button. We have a picture of this soon I think. And then you would get into the, like, user interface for that virtual machine, and you would log in that way.

Q. So, we do have a picture. It's the next slide. Let's look at the next slide, please. This is Government Exhibit 96. What is this showing?

A. So this is a picture just from the internet I took to show this. So, here you would input the IP address if you were going to do this on DevLAN. You would have to put the IP address or the host name of the ESXi server. And then your user name would be either root or your DevLAN user name. And then you'd have to put in your password and you'd click log-in.

Q. Let's go to the next slide. This shows Government Exhibit 97. What is this showing?

A. This is a picture taken from the internet. I was unsuccessful in finding a good picture of the vSphere desktop application to illustrate this. So, this is a picture of the

VMware vSphere web client which was also in use on DevLAN. The information displayed is going to be almost identical.

When you would log in through vSphere, on the left here, under Navigator, we can see you would be displayed with a the name of the ESXi server and the virtual machines that were inside that server.

Now, just to remember, this is a demonstrative from the internet. This isn't an actual picture from DevLAN.

If you wanted to, for example, go to the Confluence virtual machine, you would click on it, in this case, the selected VM in this example is called standalone. And this will show you the information about that machine. So you get detailed diagnostic information like how much storage it has, how much memory it has, how much CPU it's using.

And if you click this box here, this will give you that shell session to the server. So you would essentially click on this, and it would pop up another window, and you could just type into that window and access the server that way.

So when I say you're logging in through vSphere, this is what I mean.

Q. Let's go back to the DevLAN files. If we go to the next slide, please. This has two exhibits, 1209-17 and 1209-20. Where are these files from?

A. These files are from the ESXi server.

Q. Where on the ESXi server are they from?
A. In the log folder in a log file called host D.0.
Q. We saw that earlier. What types of things does the host D file show?
A. The host D file, among other things, shows log-ins and authentications through the vSphere and vCenter services. So if you made a log-in through vSphere, like I illustrated in the last two slides, that type of log-in will be in this log file.
Q. So let's zoom in on the top, please. What is this showing?
A. This is showing a log-in for the user root from the defendant's workstation IP address logging into the ESXi server through vSphere. We know it's that because it says as VMware client. And its time stamp is 4/18, 3:12 Zulu. So that's 11:12 a.m. on 4/18.
Q. How do you know this is a root log-in?
A. It says user root, so we know that's the root user. We also know when the, in this case the user's attempting to access the INF Confluence virtual machine. The user name of that access is also logged here as the root user.
Q. If he wasn't logged in as root, how would it appear on this screen?
A. As we had in a slide a few slides ago, if he was logged in as like a DevLAN user, it would say DEVLAN, all caps, slash and then that user's user name, in this case DEVLAN/schuljo.
Q. Do you see there a DEVLAN/Matt?

A. Yes.
Q. Is that what you're referring to?
A. Yes, that is.
Q. Let's zoom out. When was this session logged out of?
A. This session ended on 4/18, it is the lower session here, at 1:47 p.m. EST.
Q. Can you circle on the bottom session the IP address.
A. Yes, I can.
Q. The IP address ending in 165 relates to what computer?
A. This is the defendant's DevLAN workstation.
Q. What types of privileges do you need to log in as root?
A. Administrative. Server administrator privileges.
THE COURT: Mr. Laroche, would this be a convenient place to break?
MR. LAROCHE: Yes, your Honor.
THE COURT: We're going to break now, ladies and gentlemen. Remember my standard instructions. Don't read anything about the case, don't talk about it, don't do any research. Keep open minds. And leave your notebooks here. We'll see you tomorrow morning at 9 o'clock.
(Jury excused)
(Continued on next page)

THE COURT: Anything to take up?

MR. LAROCHE: Not from the government, your Honor.

MS. SHROFF: Your Honor, can I just have a minute?

THE COURT: Yes.

MS. SHROFF: Thank you.

(Pause)

MR. ZAS: Your Honor, we just wanted to flag something. We haven't made a final decision, but it might be useful, since this is a lengthy witness, for the Court maybe to give an instruction, just a normal instruction on experts in the middle of, trial. Rather than to wait until the very end.

THE COURT: What would it say? The standard instruction on experts?

MR. ZAS: Essentially, yes. We could propose something if that would be easier in writing. We can give you something tonight.

THE COURT: All right. You gave me request to charge. Is it in the requested charges you've already given me?

MR. ZAS: I don't think --

THE COURT: I know I have a charge on experts.

MR. ZAS: I don't think we had something specific in our request. But, we can give you something short and uncontroversial I think.

MR. LAROCHE: We provided a proposed --

THE COURT: I know somebody did. I don't know whether

it was the government or Mr. Schulte. Or maybe both.

MR. LAROCHE: I know that the government has, your Honor.

THE COURT: All right. I'll take a look at it. Do you have any objection to a charge?

MR. LAROCHE: No, we think one should be included in the jury charge, your Honor.

THE COURT: No. I mean, they request a charge now.

MR. LAROCHE: We have no objection, your Honor.

THE COURT: All right. Ms. Shroff, I note that today was an open session, and the courtroom is not closed. Nobody from Federal Defenders appeared.

MS. SHROFF: They did. They appeared in the morning, they were turned back so they never came back.

THE COURT: In the afternoon I was referring to. Tomorrow morning as well.

MS. SHROFF: I didn't inform them, your Honor. I ran out of time to inform them. The other two times they wanted to come, they were not allowed in. But frankly, I'm not really sure this is the witness somebody would want to see. No disrespect. But --

THE COURT: I don't know which ones they'd want to see, but the courtroom will be more open than closed now.

MS. SHROFF: But would you want to sit through that?

THE COURT: Any time they want to come over, they're

more than welcome.

MS. SHROFF: Can they come over for the next witness?

THE COURT: No, it's closed. The next witness after that will be open, they're more than welcome.

MS. SHROFF: Our objection is to the fact --

THE COURT: I know. You've objected all the time.

MS. SHROFF: Thank you, your Honor.

THE COURT: Thank you.

(Adjourned until February 12, 2020, at 9 a.m.)

INDEX OF EXAMINATION

GOVERNMENT EXHIBITS