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

UNITED STATES OF AMERICA,

v. 17 Cr. 548 (JMF)

JOSHUA ADAM SCHULTE,

Defendant.

Trial

----------x

New York, N.Y.
June 21, 2022
9:05 a.m.

Before:

HON. JESSE M. FURMAN,

District Judge
-and a Jury-

APPEARANCES

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

JOSHUA A. SCHULTE, Defendant *Pro Se*

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

Also Present: Charlotte Cooper, Paralegal Specialist

(Trial resumed; jury not present)

THE COURT: You may be seated.

Good morning. Welcome back.

MS. SHROFF: Good morning.

THE COURT: I was told that Mr. Schulte had some things to raise but was discussing them with the government first. So I gave you a few minutes, but we are pushing when I would like to start with the jury. They're all here.

Mr. Denton, do you have anything to discuss, or Mr. Lockard?

MR. DENTON: No, your Honor.

THE COURT: Mr. Schulte, anything that needs to be discussed before we start today?

MR. SCHULTE: Yes. I have several issues, but I think, hopefully, between now and the next break, we can work it out with the government.

So I just had two, two things then. One was regarding Leedom's exhibit, his expert exhibit that will be introduced here. Like I said, it was completely, basically, redone and given to the defense basically the day or two before he began. I think the biggest issue, the biggest difference is he goes into significant detail about the types of files that were deleted. That wasn't included in the previous presentation, and so it's very -- it would be very important, and the only way I can cross on the types of information in those files is

to be able to show the actual log files themselves. And so I -- you know, even if those come in as classified exhibits, I think it's very important to be able to present those files to him, because otherwise, he's not referencing any manual from the manufacturer, ESXi, or anything. He's basically testifying in his presentation that they log certain types of data, which they don't. So the only way I can cross him on that is through those logs.

THE COURT: Mr. Denton.

MR. DENTON: A couple of things, I think, are incorrect, your Honor.

First of all, that discussion of what is in those log files was in Mr. Leedom's presentation from the last trial. Mr. Schulte just raised that with us this morning. We don't have a copy of it here, but at the break, we can certainly point him to where in the old presentation this information was.

Second, we have been giving Mr. Schulte drafts that included these slides since well before the trial began, so I don't think there's a complaint that he's just learning of this now.

Second, Mr. Leedom is not testifying based on his sort of review of these files. He's testifying based on his expert knowledge of what these types of files record. There's no basis to offer large volumes of irrelevant files, particularly

given that what we're talking about are deleted files. So it's what this type of file would record, not what this actual one recorded, because the actual ones are gone. So I think, again, to the extent Mr. Schulte wants to cross-examine him about what a host D log would contain, there's no need for a classified exhibit for that purpose.

THE COURT: All right. And will you get me a copy of the original version at the break as well.

MR. DENTON: I think we can do that, your Honor.

THE COURT: Great. Assuming there's no material difference between the two, then there's no issue to raise. At this point it's very, very untimely.

Next.

MR. SCHULTE: OK. Like I said, I think the rest, most of the rest of the issues I'm giving the government a letter, and hopefully we can work those out.

THE COURT: Just tell me what needs to be discussed now, because I want to get the witness on the stand and the jury back in.

MR. SCHULTE: Yeah. So, the only -- the last thing that I had is regarding the objections. So I know that the Court has said that your typical protocol is, you know, just "objection," potentially just one word.

So I've been having a lot of problems on cross because when there's objections raised, I'm not entirely sure as to why

it is, and so I'm having problems rephrasing the question. So I was just asking the Court if there's any way that the government could just basically say the one word as to what the objection is so that I properly understand the issue.

THE COURT: Sure. Why don't you give it a shot, Mr. Denton, Mr. Lockard. Not a requirement, but a request.

All right.

MR. DENTON: Understood, your Honor.

THE COURT: All right. Let's get the witness, and then we'll get the jury back in and get going.

PATRICK THOMAS LEEDOM, resumed.

THE COURT: Counsel, I don't seem to have a name key today. Is that because it's not necessary with this witness?

MR. DENTON: It by and large should not be, but we've got it, so we're happy to produce it again.

THE COURT: All right.

Good morning, Mr. Leedom.

THE WITNESS: Good morning, sir.

(Continued on next page)

(Jury present)

THE COURT: You may be seated.

Good morning, ladies and gentlemen. Welcome back. I hope you had wonderful long weekends. It was certainly mostly beautiful weather.

A couple things. First, you've now met Ms. Smallman, my regular deputy. I expect you'll be seeing a lot more of her. We may have Mr. Lee from time to time just standing in, but hopefully, Ms. Smallman will be here for most, if not all, of the duration of the trial and you'll get to know her. She's wonderful.

We will pick up where we left off -- with the direct testimony of Mr. Leedom.

Mr. Leedom, you may remove your mask at this time. I'll remind you you remain under oath. I'll also remind you to please make sure you speak directly into the microphone, and loudly, clearly, and slowly.

With that, government, you may proceed.

MR. DENTON: Thank you, your Honor.

DIRECT EXAMINATION CONTINUED

M6lWsch1 Leedom - Direct

BY MR. DENTON:

Q. Good morning, Mr. Leedom.

A. Good morning.

Q. When we broke on Friday, you were describing some of the

conclusions you reached as a result of your forensic analysis in this case?

A. Yes.

Q. Just to remind us, what conclusions did you reach about where on DevLAN the material that WikiLeaks called Vault 7 came from?

A. It came from the March 3 Confluence backup.

Q. And what, if any, conclusions did you reach about the defendant's activity with respect to those backups?

A. So, on April 20, the defendant accessed the Confluence virtual machine, and then he reverted that virtual machine to a backup that was taken on April 16, right before the infrastructure branch had changed all those admin passwords. This gave him admin access back to the machine, and it stayed in this reverted state for a little over an hour, during which time he copied that backup file. After that, he deleted a lot of log files from the server that ran that virtual machine. It's called the ESXi server. And then he restored the virtual machine back to its currently running state, which wiped out all activity that would have occurred on that virtual machine over the last hour.

Q. Mr. Leedom, how soon after the first WikiLeaks disclosure did you become involved in this investigation?

A. It was a few weeks, late March, maybe -- maybe early April. It was a couple weeks after the investigation started.

Q. When you first started your forensic analysis, was the defendant the only suspect you considered?

A. No, absolutely not.

Q. What was the nature of your role in the first instance?

A. So, when I first got there on site, like I said on Friday, I supported the incident-response team at the FBI. So my main role there was to do incident response, you know, try and help the agency out, try and figure out what happened, try and just investigate the network and see, you know, if they had been, like, breached by a foreign actor, or if it was an insider threat. That's the role that I played working on the case for the first few months, and it was, you know, pretty unbiased, just trying to figure out what happened on the network, looking at everyone, looking at the admins on the network, just trying to understand what happened.

Q. When you say investigate the network, what does that involve?

A. So, the FBI had people on site that were, you know, imaging computers. That's something you do for forensics. You have to -- you can't just take the computer and start looking at it. They make a, like, what they call a forensic image. It's an immutable copy of the computer so you can't, you know, accidentally delete a file, for example.

As that data was coming in from the network, I helped out and we would review those machines for everything, like

evidence of intrusion, what content was on the machines, try to build out, like, a time line of kind of what happened over the network.

Q. Are you familiar with the term "finding the normal"?

A. Yes.

Q. What does that refer to?

A. So, in incident response, that's kind of the term that we use to kind of give the broad, like, strategy for investigating an incident. Because, especially on larger networks, it's not feasible to review, like, every single machine.

In this case, it's a little different because we did go through, like, every single device on that network. But normally you're only on site for a week or so, so you have to baseline the activity that's going on on that network. Obviously, for a development network that makes, like, CIA hacking tools, the normal's going to be a little bit different than, maybe, a business that, you know, primarily works with Excel spreadsheets every day. So that baseline of what normal activity is helps you know when you see something that is, you know, for a better choice of words, like, weird, you can know, like, whether that's something that's expected to be there or that's something that you should take as suspicious and we'll call it, like, pivoting into a different area of the investigation. So it's a way to kind of like guide the investigation so you can figure out, you know, exactly what,

you know, malicious or bad behavior on the network is supposed to be.

Q. Did there come a time when a particular group of DevLAN users became a focus of the investigation?

A. Yes.

Q. What group was that?

A. So, pretty early on, as kind of normal, when we do these, we try to figure out what different types of people are using the network, like, what types of permissions they have. So the administrator users for the network were kind of, like, top on the list of people to investigate both for insider and, you know, if their accounts had been, like, compromised or something and that could have been used to access data. So that user's kind of the first place to start looking.

Q. And did that include the defendant?

A. Yes, it did.

Q. How did you come to ultimately focus on him in particular?

A. As we started investigating -- like, I don't even think -- like, personally, I looked at his actual material for at least a few weeks. You know, I was focused on other material, but as we time lined the incident, started looking for things that fell outside of that normal, the only activity that looked suspicious kept pointing back to Josh Schulte, and even reviewing, like, all the other admins, all the other developers, there were very few things, if any, that, you know,

looked very suspicious. But when we were reviewing Schulte's machines, the machines he had access to, the machines he logged into, the logs from his sessions on those devices, we found some very suspicious things.

Q. Mr. Leedom, there's a binder up on the rail there. Can I ask you to take a look at that?

A. Yes.

Q. It contains what's been marked for identification as Government Exhibit 1703.

A. Yes.

Q. Do you recognize that, sir?

A. Yes, I do.

Q. What is it?

A. This is a presentation that I put together to kind of go over the incident.

Q. And will it assist in explaining your methodology and your conclusions?

A. Yes, it will.

Q. Are some of those conclusions based on exhibits that are very lengthy?

A. Yes. Yes, they are.

Q. What types of exhibits?

A. Many forensic exhibits. They could be, like, you know, a thousand pages in length, so we show the, like, the appropriate sections for the logs that we're looking at that have to do

with the time stamp that we're reviewing.

Q. Would it be difficult to display those log files in their entirety here in court?

A. Absolutely.

Q. And does your presentation summarize relevant parts of them?

A. Yes, it does.

MR. DENTON: Your Honor, the government offers Government Exhibit 1703.

THE COURT: Any objection?

MR. SCHULTE: No objection.

THE COURT: All right. Tell you what. Ladies and gentlemen, I'll certainly allow it to be displayed to you during Mr. Leedom's testimony, at a minimum, to aid you in understanding his testimony. I'm going to discuss with the lawyers later whether it should be admitted and Mr. Schulte whether it should be admitted as an actual exhibit, and I'll let you know, but in the meantime, you can certainly follow along with the exhibit.

You may proceed, Mr. Denton.

MR. DENTON: Thank you, your Honor.

Ms. Cooper, if we could put up page 1 of 1703.

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

A. Yes, it is.

Q. Broadly speaking, what are the kind of major parts of your

presentation?
A. So, it begins with kind of an overview, so we'll talk about just some basic kind of computer terms, basic overview of the network, kind of, just kind of lay a, lay a baseline for a, for the rest of the presentation. Then we'll start looking at the actual WikiLeaks publication and some information that we gleaned from that as well as, after that we'll get into some of the time lining activity and logs of what the defendant did.
MR. DENTON: Go to page 2, Ms. Cooper.
Q. What do you mean when you refer to a basic overview of the network, Mr. Leedom?
A. So, just a simple overview. There are network diagrams in evidence that are kind of complicated, so I tried to make one that was a little bit easier to understand that kind of captured all the main points.
Q. What kind of materials did you review to get an understanding of the DevLAN network?
A. A lot of things. They're -- like, it's an accredited network, so there has to be a lot of documentation for doing that. So there's, like, security documents that talk about, like, policies on the network. There's documents that have kind of like network maps of all the different machines and things like that, as well as speaking with some of the admins and asking questions to the CIA about how stuff worked, kind of generally how it works.

Q. Let's talk about some of the component parts of the DevLAN network.

MR. DENTON: Could you go to page 3, Ms. Cooper.

Q. What do you mean by network hardware here, sir?

A. This is just essentially all of the pieces of computers and computer parts that are on the network.

Q. And so tell us about computers and servers.

A. Sure. So, you have workstation computers. These are all, like, desktop workstations that, you know, you would normally expect to see when you go into the office. You've got monitor, keyboard, computer. Then there's also servers. So, these are, like, essentially like big computers. They have, like, lots of processing power and they can run applications, and we'll get into virtual machines. Some of them ran virtual machines.

Q. What's the difference between a computer and a server?

A. The biggest difference is, like, a commuter you're going to sit down to, like, at your desk with a monitor. A server's going to sit in a room somewhere, in a call it server rack, and it's just essentially a really beefy version of a computer.

Q. How do computers and servers identify themselves on a network?

A. There's two main ways. So, users can, like, write a name. So you can give your computer a name, like Pat's desktop, for example, as well as they use IP addresses, which are short strings of numbers that the computers use to talk to each

other.
Q. Moving down the list here, what are switches?
A. So, switches are how those computers are connected together. So, for a computer to be able to talk to each other, especially in, like, an air gapped -- we'll call it an air-gapped network, like DevLAN, there's no wireless. So you don't have, like, a laptop with wi-fi. You don't have a cell phone or anything like that. Everything's hardwired together with either, like, fire optic cable or just ethernet cord. So switches are just how you connect all those computers together.
Q. Explain a little more about what you mean by an air-gapped network.
A. So, in most government networks, especially government networks that deal with classified information, it would be a big security vulnerability to have, like, a wi-fi access point that was broadcasting access to the network to someone who was, like, outside the vault. That would be bad. So they're all, you know, not connected to the internet. There's no wireless connections. They're kind of, like, secure and closed off.
Q. Continuing down, what are firewalls, sir?
A. So, firewalls are just an -- they're an access control for the network. They essentially say, like, you cannot go from point A to point B or you're allowed to go from point A to point B. They just limit what computers are allowed to talk to other computers.

Q. And do they limit other kinds of traffic between computers?
A. They do. You can get pretty granular, so if you wanted to say, like, this computer is not allowed to view, like, web pages and like, like, Chrome or Firefox, like, in the browser, like, you don't want it to view web traffic, you can actually, you know, deny that at the firewall. And there's a lot more you can do as well, but the basics.
Q. And then finally, what about routers?
A. Routers just connect different networks together. I don't think we'll talk about them too much today, but --
Q. Now, we're talking here about DevLAN. Are these components that you've described unique to DevLAN?
A. No.
Q. And what about sort of the principles of their operation that you've been describing; are they unique to DevLAN?
A. Nope. The way the DevLAN network, you know, functioned at a core is similar to other corporate networks, and even, like, maybe your home network.
MR. DENTON: Go to page 4, Ms. Cooper.
Q. What does this depict, Mr. Leedom?
A. This is that simplified diagram that I mentioned earlier. We're going to start filling out pieces of this as we go through some of these slides, but this is just a basic overview of the different pieces of the DevLAN network as they relate to the case, just kind of show you.

Q. So just starting in the top left corner, explain to us what some of these pieces are.
A. Sure. So, all of the main servers are boxed here. So this one on the top left, it will make more sense as the things running on this server get filled in. But this is essentially a server that runs a bunch of virtual machines, just runs applications.
Q. And then to the right of that, what's that?
A. This is another server. This ran the Stash or, like, the code repository as well as another application that handled permissions and authentication.
Q. And then what's depicted kind of in the middle here?
A. So, this, that has the lines going to it, this is a switch. This is just to show that this is all connected together.
Q. And then down at the bottom there's a box marked DevLAN users.
A. Yup. This is just to show all of the computers, just in aggregate, that people used on the network for development, just showing that this is connected to these other services; they can access them.
Q. And all of that is surrounded by sort of the set of dots on the left, sort of two-thirds of this image. What is to the right of that?
A. Yes. So, in gray here, this is -- we call it the Hickok server. It's defined as, like, a DMZ, which is a demilitarized

zone. What means -- basically it was a single server in no man's land between the operational group's network and the developers' network, where they hosted a service that was kind of like a ticketing service. We'll talk a little bit more about it later, but it's just a way for the operators to submit, like, bug reports for projects and things like that.

Q. And what are the two images in blue and green to the right and left of the Hickok network?

A. So, these little brick walls are firewalls. The access to that DMZ is restricted, and that's just showing that.

MR. DENTON: Could we go to page 5, Ms. Cooper.

Q. Mr. Leedom, what is an operating system?

A. So, an operating system is essentially just the software that runs on top of your computer.

Q. What types of operating systems were running on DevLAN?

A. So, on DevLAN -- on DevLAN we had Windows, MacOS, and Linux.

Q. What are some of the reasons for choosing one operating system as opposed to another?

A. So, most users would have at least one Windows machine, just for productivity, like Office and things like that as well as doing code development. If you were doing code development for, like, a Mac target system, you would need a Mac to test it and work on it.

Same goes for Linux systems. If that's your target, then

that's probably where you're going to be doing most of your development. A lot of users would have a Linux system. It's just a, a more, like, you know, tech-savvy operating system. The way you access it, the things you can do are a little bit more broad than what you can do just with, you know, a mouse and keyboard on Windows.

MR. DENTON: If we can go to page 6, Ms. Cooper, and look at this diagram again.

Q. Can you explain, Mr. Leedom, a little bit about where those different operating systems were running on DevLAN?

A. Sure. So, I'll start with the bottom left, where it says DevLAN users. So, we have pretty much everything represented there. These are just users' workstations.

This ESXi server itself in the top left, it's a form of Linux. I'll describe it a little bit more when we talk about virtualization.

The Stash server as well, it's a Linux server. And I believe Hickok was a Linux server, though I'm not 100 percent sure.

Q. Are those operating systems transferable as someone who is a skilled Windows user also able to be a skilled Linux user?

A. Not likely. It depends. You would have to have experience on that, like, ecosystem and environment. A lot of activities you would be doing in Linux are what we call on the command line, where, if you've ever seen, like, the Matrix or other

movies where you have, like, a hacker typing into a black screen with green text on it, that's kind of like what that means. So you have to know a lot more about what you're doing to make use of that.

MR. DENTON: If we could go to page 7, Ms. Cooper.

Q. Mr. Leedom, you mentioned virtualization just a minute ago. At a very basic level, what is virtualization?

A. So, it's essentially just running a computer on top of another computer, or inside of another computer.

Q. So the computers that we were just looking at in that simplified diagram, were those physical computers?

A. Yes.

Q. And so you mentioned that there were also virtual machines running on DevLAN?

A. Yes, there were.

Q. So explain a little bit about how that works.

A. So, you can -- this is something that you can do, like, even for free. When you go home you can actually download some software. VMware is a developer. They create some software that lets you install, like, a little minicomputer inside of your operating system. There's some screenshots in here to help explain it, but basically you just have another little window that's on your computer and you click into it and you're using a completely different -- different computer.

Q. You've got here a reference to VMware ESXi servers. First

of all, is that a reference to a brand name?
A. Yes. So, so, like I said, VMware is, like, a brand. It's just a product.
Q. And what is a ESXi server?
A. So, ESXi is the name for their operating system, which you would install on a server, which its entire job is to run virtual machines. We call that a hypervisor in the industry. And this diagram on the right with the little blocks kind of shows how it's set up. So the blue hardware block would be your server. I'll refer to it either as the OSB server or just the ESXi server. And on top of that you have VMware ESXi installed, your hypervisor, and we'll see a picture of what it looks like. But you just have -- you could have 20, 30, a hundred different computers running on that server that people could go into and use just like a normal computer. It's just all virtualized.
Q. What are some of the reasons you might want to use a virtual computer?
A. Especially on a network like this, I think there's two main reasons that I'll kind of bubble up here. The first one is for, like, production software products. Like if you run a product, like, like a wiki like Confluence, you want it to have really high availability. So you want it to be on all the time. You don't want it to crash. If you want to make a change to it, you don't want to -- like, if you made a mistake,

you don't want to, like, completely hose the system. So virtual machines have some features which are called taking in snapshots, which are essentially, like, taking a picture in time of a virtual machine, and you can go back to that whenever and everything -- the state, like, if you had a window open on the virtual machine and you took a snapshot, and then you closed the window and you went back to the snapshot, the window would still be open. So it's just as it was when you took that, so whatever the date is on that is when you're going back to. They help out with availability.

If you needed to, let's say you had ten users using your service and you suddenly had a hundred users using it, you can very easily give the server -- give the virtual machine some more, like, processing power so it can handle that.

And then the second reason for a development network, for tools like this, when you're doing, like, malicious changes to a computer, it's really helpful to do it to a virtual machine that you can just destroy and bring back up as you test your tools. So this was primarily used to host just a few of those production services as well as development environments for the users.

Q. And then, Mr. Leedom, you've got a sub-bullet here for VMware vSphere. What is that?

A. So, vSphere is the application that you use on Windows to access this virtualized server and all of the machines in it.

We'll see some logs from that, and it's important to know what application the logs are coming from, because when you, like, click buttons to, like, start or stop virtual machines, that stuff's logged, and the vSphere application is the application that's used for that.

Q. Let's take a look at an example.

MR. DENTON: If we could go to page 8, Ms. Cooper.

Q. First of all, Mr. Leedom, is this picture taken from the DevLAN network?

A. No, it's not.

Q. What is this?

A. This is just a picture I've grabbed off the internet just to show kind of what vSphere looks like.

Q. And what does this picture depict?

A. So, the first time you'd open up the application, you'd have to type in a username and password to authenticate to the server. Without this, you wouldn't be able to access any of these machines. And then you'd log in.

Q. And there's a reference in the text in the gray in the middle to a host. What is a host?

A. A host is just another name for, like, a server that's running this software.

MR. DENTON: If we could go to page 9, Ms. Cooper.

Q. Again, Mr. Leedom, is this picture here taken from the DevLAN network?

A. No, it's not.
Q. Where is this from?
A. So, this is another just demonstrative that I pulled off the internet. It's a little bit different than what would be displayed on the DevLAN network. You can see the top, this says vSphere web client. So for this one you'd actually, like, go to a web page to log in. Something similar to this was also running on the network, but the point of this demonstrative is just to show you the different pieces of what you'd see if you were logging in to that server.
Q. Explain a little bit about what's depicted here, sir.
A. Yeah. So, let's take a look at just the first circled orange section on the left. This just shows your server and all of the different virtual machines that you could access.
Q. And then what's to the right of that?
A. Yup. So, if we move to the right, once you click on a virtual machine -- like I said, these aren't DevLAN machines. This is just from the internet. So in this case this is, like, the standalone dash numbers machine. It tells you a little bit about what's running on it. If you see where it says host with a little penguin, that's just a representation that it's a Linux machine. And this big black box is important. So if you want to, like, actually go into the machine and use it and use your mouse and type into it, you just click this box and it will pop up essentially, like, a little monitor and you can see

into that and work on it. You see a little stop button at the top there. That will turn it off. There's also a way to do snapshots. There's a snapshot tab. So if you want to take a snapshot of it to save for later, you can do that as well.

MR. DENTON: Your Honor, my monitor here has been going in and out. It's fine for me. I just want to make sure that no one else is having any issues.

THE COURT: It's fine with me, but any juror raise your hand if your monitor's having some issues.

All right. It looks like everyone else is OK, so just plow ahead and we'll try to fix that at the break, perhaps.

MR. DENTON: Thank you, your Honor.

Q. You made reference, Mr. Leedom, to that snapshot tab, and I think you started explaining a bit about that earlier. Tell us more about how snapshots work and what they're used for.

A. They're primarily one of the main reasons you use virtual machines. Let's say you want to update a piece of software, and it's a production system. You can take a snapshot before you do that in case your update goes, you know, horribly wrong or it doesn't add the futures you wanted, and it just essentially gives you a safe fallback in case you make a mistake or otherwise, and you can roll back to your snapshot and everything's working just like it was before.

MR. DENTON: Let's go to page 10, Ms. Cooper.

Q. What is the Atlassian suite?

A. So, these are those production services that I mentioned that are running on DevLAN. Want me to go through them one by one?

Q. Please.

A. OK. So, the Confluence server is the main one we're going to be talking about today. This is essentially like a wiki. If you've ever been to Wikipedia on the internet, it's going to be really similar. It's just a way for users to share information with other users. It was used for, you know, tracking work on projects and many other things. There will be some pictures of it later.

Next we have Stash. This was the code repository for DevLAN. A code repository is, like, in programming terms, it's just a place where all of the source code goes. It uses something called version control, which, to put it briefly, it's just a way for, if I, you know, write a new change to the code, I save that change and it's, you know, marked as me making the change. That way if there's an issue with it, or let's say it creates a problem, it's easy to go back and see, like, OK, Pat made that change so we're going to need to roll back the code to before he made the change, things like that. It's really helpful when you have multiple people working on a project at once.

Bamboo we won't talk about too much. This is what's called a continuous integration system. It's just a way to

automatically test code, so it just runs it for you and gives a report on how your code ran.

Jira, which I mentioned earlier, this is ticketing software. So if I have an issue, I literally can go in and post an issue, and one of the developers that owns this project can, you know, help me, you know, figure out what the bug is and fix it.

And the last one is Crowd. This handles permissions for the whole suite, which just means what users are allowed to access what different services.

Q. How would users access these different parts of the Atlassian suite on DevLAN?

A. So, throughout all this, you access through your web browser. So the same way you'd go to, like, Gmail.com, you'd just bring up a web browser and type in the address for Confluence or one of the other services, and you'd go to it in your web browser and click around, sign in. It's very similar.

Q. I think you said earlier that DevLAN was not connected to the internet, is that right?

A. That's correct.

Q. So if DevLAN was not connected to the internet, where were users going to through their web browser?

A. So, instead of typing, like, www.google.com, you would type, like, confluence.devlan.net, and the network knows what that means and routes you to the appropriate place.

Q. And what was running those web services?
A. So, Confluence, for example, was running on that ESXi server. This was a virtualized service. Stash and Crowd were actually running on what we call bare metal, so not virtualized, just running on a server.
Bamboo was also, like, a virtualized service.
MR. DENTON: If we could go to the next slide, Ms. Cooper.
Q. Mr. Leedom, help us understand a little bit about where on the diagram that you showed us earlier those particular services were running?
A. Sure. So, for virtualized services, just up here on the top left, you can see Confluence, the little globe; Bamboo, and then what I have to represent different users, like development VMs that they would use. When I say VMs, it's just shorthand for virtual machine.
Next to it we have the Stash server. Like I said, that's bare metal, so just a computer running Linux that had Stash and Crowd running on it. And then similarly for Hickok running Jira in the gray.
Q. To take an example, when you were just talking about the code development process in Stash, would a regular user working on code be logging in to the Stash server?
A. You would log in with your user account, so, like, if I had an account on the network for, like, pat@devlan, I could log in

to the Stash server through the web browser, and I would see all the projects that I'm working on from a, like, technical, programmatically perspective. When I'm, like, writing code and I want to make a change, the process, for, like, pushing that code up, I just have to provide those credentials and the name of the server and things like that, and it would send it up.

Q. Is there a difference between logging in to the web services for these Atlassian programs and logging in to the actual servers they're running on?

A. Absolutely.

Q. What's the difference?

A. So, if you're just logging in to, like, the web service for Stash in your web browser, you couldn't go into the actual computer that's running it itself and, like, turn it off, for example. You would have to access it by different means, which used, like, different passwords, different means of access.

MR. DENTON: If we could go to the next slide, Ms. Cooper.

Q. As part of your forensic examination in this case, were you able to determine approximately how many DevLAN users there were in April of 2016?

A. Yes.

Q. How did you go about doing that?

A. So, we had access to something we call, like, an Active Directory server. It's essentially just a server that has,

like, all of the users that are on the network, and we had a snapshot, I believe it was from April -- I don't remember the exact date -- of that machine and we could just go look and literally just see, like, just go count, like, OK, there's -- I think there was, maybe, like, 180 users or so. It was less than 200.

Q. Did every user have access to all parts of DevLAN?

A. No.

Q. And focusing on the Atlassian suite in particular, did all users have access to everything in all of those tools?

A. No.

Q. What limited access on DevLAN?

A. So, there were permissions in multiple places. For normal users, you would be, like, in a group that had access to certain things, like a group for Confluence -- like, if you were an administrator for Confluence, you'd be in the Confluence administrators group. But if you didn't need that access, you were just a normal user and, you know, access to code repositories and things like that are handled on a case-by-case basis with, you know, each of the services. But Crowd is the application that kind of aggregates all of that.

MR. DENTON: If we could go to the next page, page 13, Ms. Cooper.

Q. Generally speaking, Mr. Leedom, what are access controls?

A. It's just -- limits the access that people have to the

network.
Q. And what do the bullets on this slide represent?
A. These are kind of four different main ways that access was limited on DevLAN.
Q. What is a domain controller?
A. So, I mentioned this just a minute ago on how we determined how many users there were on the network. A domain controller is essentially -- it's the same thing as, like, an Active Directory server. IT'S just a place that has, like, all the biographical data. It stores your password, things like that. So if you needed a password reset or wanted to change your username, you'd do it here. So when you logged in to your computer on DevLAN, that's where you'd do it.
Q. And what does user authentication refer to?
A. So, this just if you're going to go access Confluence on the web page, it'll ask you for a username and password. So you'd have to know what your username and password is to access that application.
Q. And then below that, what is secure shell SSH?
A. So, this is one of the ways that you would access one of those underlying servers that were, maybe, running one of these production services.
Q. And --
A. Oh, go ahead.
Q. Please explain a little bit more about what that is.

A. So, SSH, it's something we call asymmetric cryptography. You have keys. You have a -- you have two keys. You have A public key and a private key. These are essentially just big strings of cryptographic numbers that you use to authenticate to a computer.

A simple way of putting it, think of it like a lock on your door. So the actual lock that's, you know, drilled into your door, that's your public key. So you can think of any door that you want to be able to have access to, you go and install your lock on that door, and your private key is the key to the lock. So if I want to, you know, put my lock on the courtroom door, I install my public key on the courtroom door and I could use my private key to unlock it. It's -- oh, go ahead.

Q. How are those keys generated?

A. You use some software, and like I said before, they're just, essentially just big strings of numbers.

Q. And is there some relationship between them?

A. Yes. So, you can't use, like, any private key to open any public key. They are, like, cryptographically married. You have to have -- you have to have that private key to use the lock with your public key.

Q. And then, finally, the last bullet here is file share permissions. What are those?

A. So, there was a file share on DevLAN. If you've ever, like, worked at a corporate environment or even at home, like

you can have a home folder where you store your information or type of perhaps, like, another share where you and someone else want to access the same data, this stuff was permissioned as well.

Q. You said a moment ago that not all users had access to all parts of DevLAN, is that right?

A. That's correct.

Q. Did some users have access to more information than others?

A. Yes.

Q. Who were those?

A. Those were the admins, the administrators.

MR. DENTON: If you could go to page 14, Ms. Cooper.

Q. What do you mean when you refer to an administrator?

A. This is essentially someone that is, you know, given the duty of, of running or administering a certain part of the network or service.

Q. Were you able to determine what types of administrators there were on DevLAN?

A. Yes.

Q. How did you do that?

A. So, by reviewing both the different machines that are on DevLAN as well as talking to the agency and then asking them questions as we kind of performed the investigation. And just reviewing the different machines. If you look at a computer, you can see who has access to that computer.

Q. What types of administrators were there on DevLAN that are represented here?
A. Three main types. There's network administrators, server administrators, and we'll call it Atlassian administrators.
Q. And what are the differences between those categories?
A. So, the network administrators -- you've heard of ISB, the infrastructure branch. These guys just essentially keep the network running. They manage the networking hardware, like the switches, as well as the main parts of the network, like that Active Directory server, things like that.
Q. And then what about server administrators?
A. So, these are the people that have access to those underlying servers that run some of those services. So you'd be able to access the actual hardware for the ESXi or the Stash server, for example.
Q. And then finally, how is that different from Atlassian administrators?
A. So, an Atlassian administrator, I think we kind of break them up into two types. There's the Atlassian administrator that has, like, admin access to that website. So maybe you could delete someone's page or make edits to the whole website. And then you have the ability to actually log in to the machine that's running -- the virtual machine that's, like, running Confluence.
Q. What kind of administrator was the defendant?

A. So, the -- he was both a server administrator and an Atlassian administrator.
Q. And what kind of administrative power did that mean he had?
A. He pretty much had full control to all of the machines, like, running these services on the network.
MR. DENTON: If we could go to the next page, Ms. Cooper.
Q. I think you started talking about this, Mr. Leedom, about the difference between the web services and the underlying virtual machines and server hardware.
A. Yes.
Q. Can you say a little bit more about the distinction between those two kinds of administrative access?
A. Sure. So, if you were an admin just for Confluence in the web page, you could go in and make new spaces, make new pages, maybe delete or edit other people's pages, restrict people from viewing pages, things like that. But you wouldn't necessarily be able to, like, go into the server running Confluence and, like, delete the application, for example. That would obviously be something you want to limit access to. So there's different passwords, different public/private keys to access the actual, you know, computer that's running these services.
MR. DENTON: If we could go to the next page, Ms. Cooper.
Q. I want to shift gears for a moment, Mr. Leedom, and talk a

little bit about how different computers interact on the network. What is depicted here?

A. So, this is a demonstrative that I put together just as a reference. We'll see a few snippets from log files. So just kind of as a basic example, I wanted to go over, you know, how some of the processes worked for some of these computers talking to each other and just highlight some of the different key words that you might see as we go through some of the logs.

Q. Why don't you walk us through this, please.

A. So, at the top, let's start. We have a client in green on the left. This could be, like, a user's workstation. And we have a server on the right. This could be, like, a Confluence virtual machine, or it could be the ESXi server itself. The words "client" and "server," you can assign a computer whatever name you want, like human-readable name. We'll just take for this example that the desktop's called client and the server's called server.

The string of numbers below that, that's called an IP address. This is just the way that computers talk to each other. It's a, it should be in most cases a unique address on the network. So if you're assigned this 192.168.1.4 address, that's your computer. Similarly, for the server.

In this short example here, we're just going to be looking at, like, a fake message log for the client talking to the server.

So underneath the client here, we have this text in yellow, which I'll talk about in a little bit. It's a time stamp. It just says when this message was sent. The message that's being sent is just "hello world" to server 192.168.1.10, which is our server on the right here.

These little arrows in the middle just denote that it's going to the server. And the server will log that it received this message. These messages, like -- like, I wanted to convey when we look at logs on this network, they're usually coming in two parts. We'll have the logs from the machine that sent the message and the logs from the machine that received the message. In the absence of one or the other, we can use the existence of that log and the time a message was sent to receive to kind of determine what happened.

In this case, we can just see that, I think, one second later from the time stamp the server received the message with the contents "hello world" from the client.

The last, important piece I want to go over as we look at these logs is the time stamp down here at the bottom. So when you see time stamps in exhibits, they'll be broken up into a few pieces.

So the first part here is just a date. So in this case, this is June 8, 2022. There will be a time stamp. In this case, this is, you know, 23:01:1:45, and there will be a time zone. So the time zone's very important. Most logs on, like,

production servers are going to be in UTC, or, like, GMT time, so no time offset. So Z just means, like, plus zero.

So if we want to turn that into, like, Eastern Daylight Time, for example, we would just subtract four from that. So this is, what, 11 p.m. So that would be, what, eight, nine, ten, eleven -- 9 -- 8 p.m -- 7 p.m. This is would be 7 p.m.

Sometimes in a log it will actually be translated already and you'll see, like, a minus zero four zero zero. So just something that we'll see as we go through these exhibits.

(Continued on next page)

MR. DENTON: If we can go to page 17, Ms. Cooper and take a real example?

Q. We are looking here at parts of the Government's Exhibits 1209-8 and 1203-44. Mr. Leedom, explain to us what we are taking a look at here?

A. Sure.

So just briefly, we will kind of go into this in more detail later these are logs from a server. The first bucket here -- the first bucket -- the first snippet here is from that ESXi server, the server that runs those virtual machines, and this is just an example of someone running a command on that server.

Do you want me to explain what the command is?

Q. Please.

A. So after "root" and there is a colon, we can see this -- you can highlight it if you want to -- yes, the ls -al var/run/log, this is just a command, it is a Linux command something that you type into the terminal so list files in a directory. It just shows you what files are in this log directory. That's all it does.

Q. And where it says root, what does that refer to?

A. So that's the user that is running this command. "Root," in Linux terms, just means administrator.

Q. This is this command being run by an administrator?

A. Yes, it is.

Q. What is in the image below that?
A. So, like I mentioned earlier, there is kind of a client server relationship to these logs. We have some exhibits from the defendant's computer at his desk, specifically a virtual machine that he ran on the computer at his desk that actually showed the output from some of these commands. So this has been snipped but this "ls -al" command that we see up here on the server, it's the same command, this is just looking at it from the client side and we actually see the output. This is the first line of the output, we will see more later on, but this is just to show kind of what this relationship looks like.
Q. I want to talk a little bit about where these snippets come from. The top image you have got here notes OSB ESXi server shell.log fileslack. What is shell.log fileslack?
A. A little bit to unpack here. So shell.log is just the log file that logs commands that people type into their computer. That's all it does.

Fileslack is a forensic artifact for looking at deleted information from a file. So if you think of it as like a box of shoes, you have the box which is essentially the amount of space the computer has allocated to store a file and you have the shoes inside the shoe box, that's the file that you are looking at, that's the information that you type into the file. When you change the size or reduce the size of content in that file, it is like you are making the shoes

smaller but the empty space in the shoe box could store some old information and that's what we call fileslack. So essentially we are looking through the empty face in the shoe box to try and find old information that was relevant to that file and that's what we are showing here.

Q. So does this command actually appear in the shell.log log file?

A. No, it does not.

Q. And then down at the bottom there is a reference to the defendant's virtual machine unallocated space. What does that mean?

A. So on a bigger term, I will go with the unallocated space first and then we can talk about the virtual machine.

Unallocated space is essentially, whenever we see that, it just means we are looking at deleted files or files that are, you know, no longer like recognized by the computer as being on the computer. When you click "delete" on your computer, it doesn't actually go and erase the whole file, it just marks that space on the hard drive as available for use so it could be years before the computer decides to use that space again to actually overwrite it and store data. So even though, like, if you deleted an icon off your desktop, even though you deleted it, forensically we can go in and still determine what was there. It depends on some varying factors on whether the computer has overwritten that space or not but usually we are

pretty successful and going back and recovering these deleted files.

Q. Are you always able to recover data from fileslack or unallocated space?

A. No.

Q. We are going to come back to this a little bit later as you said, Mr. Leedom, but for now I want to ask you, you mentioned file Storage on DevLAN.

MR. DENTON: Ms. Cooper, if we could go to page 18?

Q. What was the principal form of file storage on DevLAN?

A. So there was, in large networks like this you will typically have something called a network file share. It is just a server that's filled with a ton of hard drives that stores lots of data. You can imagine that there is a lot of data on these large networks and people need to be able to share the data and store it securely and back it up so this, what we call the NetApp server is where that data was stored.

Q. And what is NetApp?

A. NetApp is just a company. It is a brand like Dell or HP, for example.

Q. Were you able to determine what the NetApp server on DevLAN was generally used for?

A. Yes.

Q. What were some of its principal uses?

A. Some of the main users were having home directories for

every user, so as a user on the network you would have your own spot on the file share to store whatever you wanted. There was a folder for storing completed work from the group, so once a tool was completed and delivered a copy of that would be stored in a protected folder. And then there was a backup folder for backups for these Atlassian services, so the Atlassian services being like Confluence, Stash, Jira, Crowd we have talked about earlier. For each of these services, they backed up most of them every day and there was a backup stored in a folder called Altabackups.

MR. DENTON: Ms. Cooper, if we could go to page 19?

Q. Mr. Leedom, this is another version of that diagram that you talked about earlier. Does this fairly and accurately depict the basic structure of DevLAN as of April of 2016?

A. Yes, it does.

MR. DENTON: Your Honor, the government would separately offer the diagram as Government Exhibit 1251.

THE COURT: Any objection?

MR. SCHULTE: No objection.

THE COURT: Admitted.

(Government's Exhibit 1251 received in evidence)

BY MR. DENTON:

Q. So explain a little bit about how the file storage worked, Mr. Leedom.

A. Sure. So let's talk about the Altabackups so we can, I'd

ask to draw a few lines from each of these different services down to the Altabackup folder in the bottom middle starting with Confluence --

MR. DENTON: Thank you, Ms. Cooper.

A. -- and Bamboo, and one to the Stash server itself, and then one from the Hickok server.

So this is just a representation of how all of these different applications would store their backup files on the NetApp server, so just to kind of visually show you that the Confluence, Bamboo, Stash, Crowd, Jira services, all their data was being backed up in this backup folder.

MR. DENTON: If we could go to page 20, Ms. Cooper?

Q. What does this show, Mr. Leedom?

A. These are some of the other folders that that file share had.

Q. And you were testifying just a moment ago about the Altabackups. Are those depicted here?

A. No, they're not.

Q. Why not?

A. So as backups for the production services, that was actually kept completely separate.

Q. In what way?

A. It is a completely separate, like, shared volume. It had different access controls than the normal files that people would be able to see and access on the network. Things like

that.
Q. So does this depict what a normal user would see trying to access that file share?
A. Yes.
MR. DENTON: So let's go to the next slide, Ms. Cooper, page 21.
Q. What is this, Mr. Leedom?
A. So this is how you would mount that Altabackup share from one of these production servers or services.
Q. And is that different than just clicking on a folder?
A. Absolutely.
Q. What is it?
A. So this is a file from a Linux computer. All this does -- we won't go through the whole thing -- it just says every time the computer boots up you need to mount this backup -- looking at the last line here that is highlighted -- you need to mount this backup folder Altabackup from the server 10.3.1.70 to a folder on the computer itself which is /mnt/altabackup, and we are using a protocol called NFS -- this is just network file system, we won't get into it in detail, it essentially means it is a different protocol than something you would be clicking through in Windows. And the rest of this just says how do you want to mount it? The key takeaway from the rest of this command is that you are mounting it read/write so you can write to it, you can edit it, it is not just, like, you can mount

something read-only which would just be to look at it, you couldn't edit it. Things like that.

Q. Where did this particular mount point come from?

A. So this mount point is from the Confluence virtual machine itself.

Q. Could a regular Confluence user access this mount point?

A. No.

Q. What would you have to do to be able to access this mount point?

A. So you would have to be a confluence server admin and log into the actual Confluence virtual machine itself and go in on the command line and access it that way. If you were just going in through your web browser, you couldn't see this.

Q. What about the other arrows that Ms. Cooper just drew, at your direction, on that; where were those mount points located?

A. They were, similarly, either in the -- if the application was virtualized it would be in the virtual machine or like in the case of Stash, it would be on that physical server.

Q. Now, you said this was in the Confluence virtual machine; is that right?

A. Yes.

Q. Would this mount point only let you access Confluence backups?

A. No. So the Altabackup share itself has all of the different applications backups.

MR. DENTON: Go to page 22, Ms. Cooper?

Q. What is this, Mr. Leedom?

A. So if you went into that Altabackup folder, this is what you would see. You would see a folder for each of the services that was being backed up. So this means that even if you mounted the Altabackup share on the Confluence VM, you could see the backups for Bamboo and Crowd and Jira, for example.

Q. Explain a little bit about how we would get from that mount point we were looking at as text, to this screen here.

A. So you would essentially, in the virtual machine that had access to this backup server, you would just go to that -- I think it was like /mnt/altabackup, wherever it was mounted locally on the computer you would go to that, open it up, and you could see it. But if you didn't have permission or couldn't mount this file share or were trying to mount it from somewhere else in the network, you wouldn't be able to see this.

Q. As part of your forensic work in this case were you able to determine how the backups in these folders were created?

A. Yes.

MR. DENTON: Go to page 23, Ms. Cooper? Thank you.

Q. Mr. Leedom, help us understand this Atlassian backup script here in Government Exhibit 1207-17.

A. So we won't go through the whole thing here. This is just a script that backs up the Confluence server.

Q. And, generally speaking, how does it work?
A. So there is, you know, the main part -- there is two main parts for the Confluence server. There is a database which stores a lot of information about, you know, what's on the pages, like what a user's name is and what pages they own, things like that, and then there is a separate part which is kind of like a home directory for the service which stores things like file attachments for pages. So if you took a picture of a cat and put it on your Confluence page, that picture of the cat would be stored in this home folder. So to back up this service to restore it at a later date, you would need a copy of the database and a copy of that home folder. So this script just zips up the home folder and then exports the database and then stores them on the Altabackup server to back it up.

MR. DENTON: And then, Ms. Cooper, if we could blow up the bottom three lines of the image, please?

Q. What does this show?
A. So I will walk through each line here.

So "echo" just says if you are on a terminal and you type the word "echo" and you type a phrase, it is just going to output that to the terminal, kind of like paste it out again for you. This is for logging, so when you are looking at a log you can see, OK, it is trying to copy the backups to the NFS. It says "shart," I think that's a typo, it should probably say

"share." And then we have two demands after this, this cp command stands for copy. I'm not going to read this whole thing but it says, hey, copy those backups that I just made to that Altabackup share. It also puts in, going to the middle -- can you highlight the $timestamp?

So programmatically, $timestamp is what we call a variable. It is a sign somewhere in the script; they get time and date and put it in the file so it let's you know when the backup was taken.

MR. DENTON: If we can go to page 24, Ms. Cooper?

Q. What does this depict, Mr. Leedom?

A. So if you go into that Confluence folder in Altabackup you see all the backups for Confluence. These are all of those backups as of, it looks like July 27th, 2016.

Q. And what is the difference between the two images here?

A. So the ones on the left, these are those database backups and the ones on the right is the zipped-up home folders.

MR. DENTON: Let's take a little closer look at this and if we could go to the next page, Ms. Cooper, no. 25?

Q. Mr. Leedom, I would like you to walk us through what information is shown here.

A. Sure. So we will start with the top one on the left here, we have the File Name so this top one is just the database backups. We know it is a database backup from two things; (a) we just looked at the script and know what these are supposed

to look like. You see that little db in the file name as well as ending with ".SQL," SQL is a type of database. So that essentially has the file name and time stamp.

Going through the other columns, Date Modified, this is the last time this file was written to.

Type we just talked about.

Q. What do you mean by written to?

A. So when you create this database backup, let's say it takes a couple minutes -- in this case it is pretty small, like 400 megabytes, so it may take, say, a few seconds to actually export all of that data from the database and save it to a file. It doesn't do that all at once so it finds a spot on the computer and starts writing line by line into that spot, and once it is finally done writing everything, wrapped it up, it will slap the date modified timestamp on there for when it is finished. This is just the time when the backup was finished and put on the uploaded to that backup share.

Q. And then what about Type?

A. So Type, this is just the type of file. This is based off the file extension, so that .SQL, Windows says, yes, it is a SQL file.

Q. What is a SQL file?

A. Yes. Sequel is just shorthand for SQL, it is a database file.

Q. What does SQL stand for?

A. Structured Query Language.
Q. Again, just at a very basic level how does an SQL database work?
A. So it is kind of like if you have, like, a filing cabinet, so let's imagine the entire cabinet is a database. A drawer in the cabinet would be a table in that database, let's say we have a drawer labeled, like, grocery store items so we open up that drawer and start looking through the folders and each of those folders would be labeled, like, a different fruit that you would find at the grocery store apples, bananas, etc.
Q. And then what does the Size refer to?
A. So this is just the size in bytes, how big the file is. In this case it is about 390 megabytes.
Q. Then to the right, the Date Accessed, what is date accessed?
A. So this is the last time anyone, or a service, or whatever, touched this file. So if you opened it up to read it, read the contents, if you copied it, if you did just about anything to it that's more involved than just, like, clicking on it and clicking off of it, it is going to update this date access time. So this essentially just tells us this is the last time that file was touched.
Q. How is that different from Date Modified?
A. Date Modified is the last time the file was modified. So, like, if I have a document I can read it and see what's on it

but if I, like, took a pen and started writing on it then I would be modifying and changing it so that would update the modified time. But if I just picked it up to read it, it would change the Date Accessed time.

Q. At the risk of asking the obvious, what is Date Created?

A. So this is the time that that file was created.

Q. Are those the same column headings in both top and bottom of page 25 here?

A. Yes, they are.

Q. Do you see under the bottom image where it says file type as winRAR archive? What is that?

A. This is essentially just a file on the computer that this screenshot was taken, the application winRAR was installed, it is just an application that can unzip things. The most important thing to look at here is, like before, these last four characters of the file name, this ".TGZ," this stands for -- the T stands for tarball. It is essentially just a zip file. It is a Linux version of a zip file. That's as simple as it is.

Q. As part of your forensic work on this case did you review the backup files for Confluence?

A. Yes, I did.

Q. Why was that significant?

A. Well, in looking at what got posted on WikiLeaks, we wanted to know where it came from (a), and when it came from. So we

had to review all of these backups to determine, like, what content was posted online and when that content was available on the network so we can determine, like, when it was taken.

Q. Did you identify anything unique about a particular set of backup files?

A. Yes.

MR. DENTON: If we can go to the next slide, Ms. Cooper, page 26?

Q. Which backup files were that?

A. These are the March 3rd backup files.

Q. What was unique about that them?

A. So of all the backup files, like, for Confluence on this network, the time that these two files were accessed, you can see it is different from all the rest of them. So we know that this file at 4/20/2016 at 5:42 EDT, it was either read or it was copied. That's essentially what that is telling us.

Q. Across the universe of Confluence backup files that you reviewed including those that are represented here, was there otherwise some relationship between date modified, date accessed, and date created?

A. Yes, there was.

Q. What was that?

A. They're pretty much all the same within, you know, seconds of each other. These only show, like, to the minute, but you can see, as you just look across these, especially for

Confluence which is a smaller service that didn't take very long to back up, once that backup was made and it was put on the backup server, like those timestamps they never changed because they weren't accessed. So when we see an outlier like this, and like I was talking about earlier talking about finding the normal, this is an outlier and something that we investigated as far as, like, trying to figure out how does this 4/20 5:42 date fit into the timeline.

Q. Mr. Leedom, you have been testifying about the significance of this particular Confluence backup. Did you also review backups from Stash?

A. Yes, and the other services as well.

Q. As of the time that you were able to review data, did a March 3rd backup for Stash still exist on DevLAN?

A. No, it did not.

MR. DENTON: If we can go to page 27, Ms. Cooper?

Q. What does this slide show, Mr. Leedom?

A. So when we arrived onsite, which was in March of 2017, for what we were available to review from this backup server, these backups only went back to May 1st, if you look at the very first line.

Q. How often was Stash backed up?

A. We can take a look here and you can see it was backed up daily; May 1st, May 2nd, May 3rd, etc.

Q. Generally speaking, how would you describe the size of

these backup files?
A. They are very large.
Q. And what, if any effect, does that have?
A. It means it could take a while to back it up (a), and (b) it takes up a lot of space on a file share and data storage is pretty expensive so you want to manage that.
Q. How does the size of these backup files for Stash compare to the backup files for Confluence that we were just looking at?
A. These are much, much larger than the Confluence backups.
MR. DENTON: If we can go to page 28, Ms. Cooper?
Q. Take a look at what is in evidence as Government Exhibit 706. Do you see, Mr. Leedom, the reference in the second line here to: I've found my way into /mnt/altabackup/stash?
A. Yes.
Q. What does that refer to?
A. This just says, like, hey, I've logged into a server that has access to these backup files and I'm looking at it, I found it.
Q. Then in the sixth line where the defendant says the .SQL or the database and the .TGS are the zipped home directories, is that what you were just testifying about with respect to Confluence?
A. Yes. That's correct.
Q. Was the same true with respect to Stash?

A. Yes.
Q. A little further down where the defendant says: Yeah, you can use the month, too, so RM Stash_DB-03*. What does that RM Stash language refer to?
A. This is a command that you would type into the terminal on a Linux computer. "RM" stands for remove. This basically says delete this file. It is a little special since there is a star after that 03, that's like a wild card so if you give that to the delete command it will delete every single file that starts with Stash_DB-03. So, essentially, this says delete all of the Stash backups from March.
Q. So based on your analysis of the network, did you reach any conclusions about why a March 3rd backup of Stash did not exist anymore?
A. Yes.
Q. What conclusion was that?
A. It was deleted.
Q. I want to shift gears a little bit, Mr. Leedom, and move on to the next part of your presentation.
MR. DENTON: If we could go to page 29, Ms. Cooper?
Q. As part of your investigation, did you review the actual material that WikiLeaks posted on the internet?
A. Yes, I did.
Q. What did you review?
A. So I reviewed the actual web pages from WikiLeaks for the

releases.
Q. When you say the releases, did that information come out over time?
A. Yes, it did.
Q. I want to focus in particular on the first, the March 7, 2017 leak. I think you testified earlier that you reached some conclusions about where that information came from; is that right?
A. Yes, I did.
Q. Where did it come from on DevLAN?
A. So that March 7th leak, that all came from Confluence, specifically that March 3rd Confluence backup.
Q. How much of Confluence was disclosed on March 7, 2017?
A. All of it, or at least everything that was available in that March 3rd backup.
Q. Did any individual user have access to all of those pages on the Confluence web service?
A. No, not normal users.
Q. What do you mean by not normal users?
A. If you were an administrative user for Confluence you could see all of the pages in the site, but all the other normal users would only be able to see what pages they were explicitly allowed to see.
Q. Was there something about the data posted on WikiLeaks that allowed you to say that it specifically came from a backup

file?
A. Oh yes.
MR. DENTON: So if we could go to page 30, Ms. Cooper?
Q. Is this the same script that we were talking about?
A. Yes.
Q. Was this significant to that determination that the WikiLeaks material came from a backup file?
A. It is very significant.
Q. How?
A. If we look at the -- I don't know if we can blow it up or not.
MR. DENTON: If you can go to the next page, Ms. Cooper?
A. Perfect.
So there is a command in here which I'm not going to go through every piece of it but this "my SQL dump" this just says hey, backup the database. That's all it says. There was an issue with this command, it was missing what we call an argument. We will look at this -- you see the little -u right after the my SQL dump command, we call that an argument. There was an argument that needed to be provided to this command to properly back up the type of data that was stored in this database. Essentially there was an error when the backup command hit a certain string of bytes that it didn't understand and it kind of bailed out and only ended up backing up like

three quarters of the whole database. So in technical terms we would call that a corrupted backup and the particular type of argument that is missing here is one that would correctly set the encoding for that database so that it would know, oh, I see something I don't recognize, I'm supposed to treat it like this, and keep going.

That's basically what happened.

Q. And what type of data was missing from the backup as a result of that error?

A. There were a few tables, like drawers, missing from that database. The most important one, there was a table that matched up essentially like what users and what pages were associated. So if, like, I had a page on Confluence, the table that had the information of saying, like, exactly what pages, my user name and stuff was associated and those edits were associated with, that was all missing.

Q. As part of your analysis, did you try to figure out how someone would go about reconstructing Confluence from these corrupted database files?

A. Yes.

MR. DENTON: If we can go to the next page, Ms. Cooper?

Q. Describe that process for us, Mr. Leedom.

A. Sure. So I took it to super ground level. I received these two files, I don't know what they are, let's see what I

can learn from them. So the first step would be, OK, I got this backed up zip file and some database file. I have to determine what these are. The file name is labeled "Confluence" so I can go Google "Confluence" and assume, OK, it is probably this wiki thing and trying to look for data in these two files that might show me what might have been in that wiki. One is a database so I load it up in a database viewer, look at all the tables, try and figure out what is there. When I am Googling "what is Confluence" I might run across some -- Confluence is an Atlassian product, there is actually steps from Atlassian on how to restore a Confluence backup with these two files so I tried that. It didn't work because the database was corrupted so that normal process failed.

Q. And just to be clear, Mr. Leedom, did you actually do that?

A. Yes.

Q. And did it work?

A. No, it did not work.

Q. Please continue.

A. So when that doesn't work, the only method you really have is to literally like manually go in and look at all of the data in this database and try and rebuild what is there.

Q. So let's talk a little bit about how that manual process would work.

MR. DENTON: If you can go to page 33, Ms. Cooper?

Q. What's the first step in manually re-constructing

Confluence pages from these backups files?
A. So the first step in re-constructing this Confluence database, it's the same for any database honestly, you have to understand what the database looks like, you have to know what tables are there, where things are stored. This is what we call a relational database, that means there are relationships between those different drawers in the cabinet that you have to understand otherwise you don't really know how to deal with what you have.
Q. And so once you have done that, what are the kinds of relationships that you need to identify?
A. There are quite a few. You have the actual content that someone would have typed onto a page. These pages had versions so if I made an edit to a page, it would make a new version. So if you wanted to go back to an older version of a page, for example, you could do that. So the order of how those pages are versioned are stored there. The order of where those pages are stored in relation to other pages is stored there. Let's say you have a space that just talks about Mac tools, there would be specific tools under that space that's related to Mac tools so that relationship is something that you have to understand, who owns pages, like what specific users owned or edited pages, what users commented on pages. You could literally go in and write a comment on someone's page about a project or something. What data was attached. Like I said, if

I attached a cat picture to a page in the database there would be an object for, like, hey, there is cat.JPEG, what page is it associated with, for example.

Q. Would that process have been affected by the data that was missing from those tables as a result of the error that you described?

A. Absolutely.

Q. How would that have made this harder?

A. It significantly hampers the efforts, specifically because the data that is missing is this table that relates all of these -- there is internal ID numbers for different objects in the table, they're really long, we will see some in a minute, but the thing that maps those ID numbers to the name, like Pat Leedom, like that table is gone. So all you have to work with are these unmatched relations between these long identifier numbers and it can be impossible to resolve those without the data from that table.

Q. As part of your forensic work in this case, did you try to reconstruct some Confluence pages manually in this way?

A. Yes, I did.

Q. About how long did that take you?

A. I spent about a week just going through the process and trying to figure out, OK, how did WikiLeaks do this before I came to my conclusion on what happened.

Q. Just to be clear, did you rebuild all of Confluence in that

week?
A. No.
Q. Based on how much effort it took you, would it take a significant amount of time to restore Confluence from one of these backups?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. Yes, it would.
Q. Would that process restore Confluence to the way it actually looked on DevLAN?
A. Absolutely not.
Q. What would be different?
A. We will have, I think, some pictures, but the whole site would look different. There would be data missing, there would be, like, obvious gaps where, you know, you would have to re-interpret how some of these relationships worked and you might get them right in some parts, you might get them wrong in other parts. So I looked at those errors and inconsistencies to try to determine how this was done.
MR. DENTON: If we can look at page 34, Ms. Cooper?
Q. Does this summarize some of what you found analyzing what was on WikiLeaks?
A. Yes.
Q. Explain a little bit more about this for us, Mr. Leedom?
A. So the biggest, most interesting part of Confluence would,

I would say at least it the content on the pages. So if I write a page talking about cats, you know, the content, all that content talking about the cats, that content is actually all stored in the database in a table, it's actually stored pre-formated and everything, actually pretty easy to pull out. So that's most of the content that is on WikiLeaks for this, is all that body content for the pages, that's where all the juicy information is.

Q. Were there other parts that reflected the errors you have been describing?

A. Yes. So, like, while the content for the pages was all there and in tact, all of the other stuff that kind of enhances what would be on those pages was missing. A lot of user IDs weren't available. A lot of pages were incorrectly associated with other page names. There were pages that were both completely missing as well as pages that if you, like, looked at it on DevLAN as it was, a page could have been completely deleted. WikiLeaks actually just restored it as it was so they actually recovered deleted pages to some extent for some of these pages. And from a, like, overall visual presentation perspective, the design elements and templates and fancy fonts and stuff, all of that is gone.

Q. So let's go through some examples of that, Mr. Leedom.

MR. DENTON: If we can go to page 35, Ms. Cooper?

Q. First of all, Mr. Leedom, where does this picture come

from?
A. So this is a demonstrative. This is just from, I just Googled "Confluence" to get a good picture to show of what a normal Confluence page looks like because ours are heavily redacted so I just wanted to be able to kind of show all of the different little pieces that go into making a Confluence page.
Q. Let's actually look at one of those pages, if we can look at the next slide, slide 36? What is this, Mr. Leedom?
A. So this is a page from DevLAN from Confluence.
Q. And how does this compare to that generic example that you were just talking about?
A. So we can see a lot of similarities; just look at the blue bar up at the top, we can see the Confluence logo, some buttons, we go down the left side here we have the space, in this case it is the operation support branch, we have pages, child pages, that's a relationship, you can see this kind of down here -- yes, exactly there. We can see under OSB home there is relationship to OSBs ESXi server so that's a page relationship that is something that is stored in the database. And then the content here on the right we see some tables, some bold headers. Even on the very bottom there is a comment box where you can write comments.
Q. Let's take a look at some of what was posted on WikiLeaks.
MR. DENTON: If we can go to page 37, Ms. Cooper and look at 7-3 in evidence?

Q. What does this show, Mr. Leedom?
A. So this is a page from Vault 7 release from WikiLeaks. I tried to find a simple page to use for an example so this is the page called "Nope" where the content is about "Making Make Suck Less." "Make" is a Linux command, it compiles code, essentially.
Q. Does some of what was posted on WikiLeaks here appear as it would have appeared on Confluence on DevLAN?
A. Yes.
Q. Can you explain that?
A. So like I briefly mentioned earlier, all of the page content that is stored in the database, it is actually stored, we will say, pre-formatted. This is a web page, the kind of programming language for web pages is called HTML. All of that data is actually stored in the database so if you wanted to, you know, preserve like these numbered bullets that are indented, this kind of quote thing at the bottom here for the code block down there, that's actually all in HTML and already formated, so all have you to do to retain all of that is just copy it out and open it up in a web browser.
MR. DENTON: Let's take a look at the next page, Ms. Cooper, no. 38.
Q. What does Government Exhibit 1207-43 show, Mr. Leedom?
A. This is exactly what I did. I just copied this page content out of the database, dropped it in a -- I just opened

up Notepad, dropped it in, saved it as a .HTML file and opened it in Firefox or Internet Explorer and you can see the formatting and everything is exactly the same as it was on WikiLeaks. The font is different. The color might be a little different because that is something that's kind of dynamically handled by the web server that is running it. So WikiLeaks has their own font and color scheme so that's just kind of superficial, but for the actual content itself it is identical.

MR. DENTON: Let's go to the next page and actually do that comparison, Ms. Cooper.

Q. Is this what you were just describing, Mr. Leedom?

A. Yes, it is.

Q. So how is the WikiLeaks content different?

A. So we can see the -- it has a different font, the color is a little bit different. This is kind of the main pieces. I didn't go through, like, the page relationship stuff for this example, this is just the body content so we don't see the, like, navigation, directory, macOSX nope, that's not on the bottom here but that's because this is just the page content.

Q. What, if any conclusions, did you draw about the fact that the page content from the SQL database rendered correctly on WikiLeaks?

A. It certainly made it a lot easier and more feasible when we are thinking about how this data was stolen and like when it got posted, this is how they did it. They had the database,

the content is all there, pulled it out, and can just make a website with it.

Q. Did other pages from WikiLeaks have information that was missing from what would be visible on DevLAN?

A. Yes.

MR. DENTON: Let's go to page 40, Ms. Cooper.

Q. What does Government Exhibit 10 show, Mr. Leedom?

A. So this is another page from WikiLeaks.

Q. What is this long string of numbers and letters that starts with FF808?

A. So this is actually a user ID number. That would be in the database, specifically one that you would find in that table that was missing. These are used kind of all over the place so it is actually possible, in some instances, to correctly find the relationship to some of these but this is one instance where it's not. So this long string of numbers just essentially is a replacement for, like, a user name.

Q. Did each individual Confluence user have a number like this?

A. Yes.

Q. How was it assigned?

A. It's, like, they're unique. I don't know exactly how they're generated, but each user has a unique number associated with it.

Q. How is this different from how the page would have looked

in Confluence running on DevLAN?
A. So this page, like as is, actually doesn't exist at all on DevLAN. One thing WikiLeaks did when they rebuilt a lot of these pages is, like, kind of created new pages to aggregate certain things like certain content from users because a lot of those previous relationships were broken so they had to have some way to try and put the pieces back together. So this is essentially, like, all of the pages or attachments that they could find that were related to this user ID string.
MR. DENTON: Let's take another example, if we could go to page 41, Ms. Cooper?
Q. In what ways is Government Exhibit 7-1 different from how this page would have appeared on DevLAN?
A. So, this page doesn't actually exist on DevLAN. Yeah.
Q. Explain a little more about that?
A. Sure.
So this page, this says MacOSX. Essentially there was a user on DevLAN that did a lot of work on Mac projects and since that user page association table was gone, the best that WikiLeaks could do with this was they thought that, oh, well this must be like a separate space for just MacOS projects --
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. -- this must be a separate space for MacOS projects and that's why they labeled it as such, and kind of binned all of

these things together when, in reality, if you had like a correct, full backup, you would know that this actually isn't a real page.

Q. Let's take a look at page 42. Did you do work to analyze Government Exhibit 7-1 in particular?

A. Yes.

Q. Explain to us what you did.

A. So this is one of those examples where I saw, OK, well this is weird. This doesn't show up like it does on the network normally so let's try and figure out why. Not only is this a page that doesn't exist, this Ghidra 6.0.10 on OSX/elcapitan page, if you look at the bottom right here, this is actually a query from the database itself, this page is deleted. So if you looked at this users list of pages on DevLAN on March 3rd, you wouldn't see this page because they a deleted it. So this is showing how WikiLeaks actually recovered some deleted pages when they rebuilt this.

Q. What is the string of text that's in between Government Exhibit 7.1 and Government Exhibit 1207-94?

A. So this is the actual query that I ran on the database to generate the table that's below.

Q. So what, if any conclusions, did you draw from the fact that WikiLeaks posted a page that did not exist and that contained deleted information?

A. So it goes to show that they weren't trying to just like

post stuff that they had, they were going through and trying to get as much out of these backups as possible so they wanted to use, like, every little piece that they could find. If there was deleted stuff they wanted to show that, they wanted to make the best use of this backup that they could and present, like, as much -- you know, we call it carving in forensics -- as much recovered information as they could.

MR. DENTON: Let's go to page 43, Ms. Cooper.

Q. Were there other aspects missing from WikiLeaks' publication of the material from DevLAN?

A. Yes.

Q. Like what?

A. So this example that we will talk about, this little red box here, it just says "details missing." If you go to this page on DevLAN, there is actually, like, a little table here with colors and, like, formatting and stuff.

MR. DENTON: Let's go to the next page, Ms. Cooper, we may be able to look at that in more detail.

Q. What does Government Exhibit 1207-93 show?

A. This is showing the actual content for an object on the page which is called Details. If you highlight the top there right under the big black line -- exactly.

So this is essentially a table that is just called Details, and we can see it's got a date, it's got a column called Participants, and it has some users listed and I think

they were, like, color-coded or something. So when WikiLeaks wrote a program to go through and recover all the data from the database backup, it didn't know what to do with this because you have to manually handle -- we call them, like, edge cases, you have to manually figure out how to handle this. So this is just another example to show, like, if you looked at this on DevLAN, it would look a lot different than it does on WikiLeaks.

Q. Is the difference that's reflected in the fact that this information is missing related to the error in the backup scripts that you described?

A. So it's less specific to, like, the corrupted database and more specific to, like, not having a way to handle these types of embedded objects that are in the database. So we see here it says Structured Macro at the top right next to the highlighted portion, so on a Confluence server it sees this and knows exactly what to do with it and it is like oh, this is a macro table and it renders it as a little colored table, but since WikiLeaks isn't using Confluence to read through the database they're doing this all manually, they just didn't know how to deal with it.

MR. DENTON: If we can go to the next slide, Ms. Cooper, no. 45?

Q. You testified that the March 7th WikiLeaks posting contained all of Confluence; is that right?

A. Yes.
Q. As part of your analysis, did you consider other ways in which an individual could obtain all of Confluence from DevLAN?
A. Yes, I did.
Q. Let's go through each of those.
A. Sure.

So, like, from a security incident response perspective just trying to think, put myself in their shoes like what are ways that you could take this. The first one is something we call a web scrape. This would be going to literally every single page on the Confluence page and just printing it out either to a PDF file, or you could print it out if you wanted to, it would be thousands of pages. But, from what we see from what was posted, that big blue banner at the top, all the formatting, all the stuff that is missing and added, we know that wasn't the case.

Q. Just to be clear, what kind of privilege would a user need to conduct a web scrape that would collect all of Confluence?
A. You would have to have admin privileges to Confluence because you would have to be able to view every single page.
Q. How long would something like that take?
A. It could take a while. It could take a while.
Q. Did you reach any conclusions about whether a web scrape was how all of Confluence was taken?
A. Yes, I did.

Q. What was that?
A. It was not taken by a web scrape.
Q. And then the next bullet here, complete VM copy. What does that refer to?
A. So we know Confluence was running on a virtual machine. You can actually export that virtual machine to a file -- it's humongous, but you can actually do that and you can move it to another computer and turn it on over there and run it. So that's totally another way that we considered that this could have been taken.

For pretty much all the same reasons as above, if you had the whole virtual machine you wouldn't have all of these errors that were clearly introduced by missing this specific relationship table from a corrupted backup. It would look very different.

Q. And again, if someone were going to try and take a complete VM copy, what kind of privileges would they need to do that?
A. You would have to be, like, a server administrator to actually, you know, admin the server that ran that virtual machine to export that whole computer out.
Q. And you said that that computer would be very large. How did that size compare to the size of the backup files that we were looking at earlier in the Altabackups folder?
A. The size of the computer would be significantly larger, like magnitude times larger. The backup of Confluence

themselves is actually not very big.
Q. Going down to the next bullet, was restoration of a complete database and home directory even a possibility in this case?
A. No.
Q. Why not?
A. Because the only backups available when we saw the script that ran every day, all of those backups were all corrupted in the same way.
Q. And so the restoration of a corrupted database, is that the process that you have just been describing?
A. Yes.
Q. What would someone need to do to be able to get a copy of that corrupted database and home directory?
A. Like, what they would need to do on DevLAN?
Q. Yes, sir.
A. So you would have to have access to that Altabackup share. I spoke a little earlier, the only place that that backup share was available was on those actual computers that were running those services and in some instances, like Confluence, you had to be on that Confluence virtual machine itself to access that backup.
MR. DENTON: Now if we could go to slide 46, Ms. Cooper?
Q. We looked at this before, Mr. Leedom, and I think you

testified that Confluence was backed up daily; is that right?
A. Yes.
Q. Does just looking at this page here, for example, the March 5th backup of Confluence, contain all the data that's also in the March 3rd backup?
A. It has different kinds of data. In general, it's pretty much going to have everything that's there. Since Confluence is a, like I said, it stores version history, most of that data will be there.
Q. So using those tools, would it be possible for someone with access to, say, the March 5th backup of Confluence, to make it look like it came from an earlier backup file?
A. It would take a very significant amount of effort.
Q. Why?
A. Because when we look at how much effort it was to actually get it restored and pull out and figure out how the database works to begin with, and the fact that you have to account for pages that are deleted, pages that, you know, what if a user left and their whole like pages are gone or it stopped getting updated and these relationships are very complex and go across multiple tables in the database, trying to restore a backup at all is very complex, much less trying to restore a backup and then fake the backup to look like an older backup, you would also have to have the older backup, too. There is no way you would really be able to know just from what is there what it

would have looked liked on March 3rd. Some pages have revision history but not all of those relationships rely on that.

(Continued on next page)

BY MR. DENTON:

Q. And you testified earlier that the date-accessed time on this particular backup was unique, is that right?

A. Yes.

Q. Did that inform your opinion about whether the data came from a later backup?

A. Yes, it did.

Q. Why?

A. Because we can look here, the only file that's been accessed in this short list -- you can look at the larger list too, but this is the only one that has, you know, a later access date. So this shows us that, you know, we know that this database backup was read or copied.

Q. And so based on your analysis of the information in the Vault 7 disclosures and then this information here on Government Exhibits 1207-27 and 30, did you form any conclusions about where the Vault 7 leak information came from?

A. Yes.

Q. What was that?

A. It came from these two backups, these two March 3 backups, from Altabackup.

Q. And again, were you able to perform that same type of analysis for data from Stash?

A. No.

Q. Why not?

A. Those Stash backups were not available.
Q. And why were they not available?
A. Because they were deleted. All the March Stash backups were deleted.
Q. We're going to move away from the leak, Mr. Leedom, and talk a little bit before specific computers on DevLAN now.
MR. DENTON: If we could go to page 47.
Q. Did you review the defendant's DevLAN computer?
A. Yes, I did.
Q. What is E0001 a reference to?
A. So, this is just -- it's not even the whole thing, I think. It's just a piece of the evidence tracking number that the FBI forensic team assigned when they imaged the device.
Q. Did all of the various devices that you reviewed have an evidence number assigned?
A. Yes, they did.
Q. Did you personally review the workstations of other DevLAN users besides the defendant?
A. Yes.
Q. Which ones?
A. A lot of them. More specifically, like, all the administrators, multiple users on the network, for sure.
Q. Let's talk about the defendant's here for a moment.
MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. What does Government Exhibit 1202-2 depicted here show?
A. So, this is just identifying information for the computer. Just came out of the -- one of the forensics tool. This is just all stored in a database called the registry on Windows. So we'll just look at a couple pieces.
The first line here, registered owner, Schuljo, this is Schulte's username on DevLAN. And then I want to take a look at the actual product here, just to show that, yes, this is a Windows computer. About halfway down, it says product name, you know, Windows 10 Enterprise.
Q. And you said his username was Schuljo at the top there?
A. Yes.
Q. Did you look at data about that username on this computer?
A. Yes.
MR. DENTON: Go to page 49, Ms. Cooper.
Q. What does Government Exhibit 1202-2 show?
A. So, this is more forensic information from Windows. This comes from the registry. This just shows all of the different accounts that were on the computer and how many times they've logged in, when they last logged in.
Q. And what's the last log-in on this computer?
A. If we look at the very last line here, it's for the Schuljo account, and the last log-on date was October 27, 2016.
MR. DENTON: Go to page 50, Ms. Cooper.
Q. What does this show, Mr. Leedom?

A. So, this is a log file from this computer that shows at a specific date a specific host name for the computer. It says that human readable name for what the computer was called, as well as at the bottom the IP address. This is that way the computer talks to other computers.
Q. And how is that host name set?
A. It's set by the user. So, you can go on and change it as a user.
Q. What name did the defendant set for his computer?
A. KingJosh-PC.
Q. And what was the IP address that was assigned to that computer?
A. It's at the bottom here, 10.3.2.165.
Q. Now, is this just an example of the IP address assigned to the defendant's computer?
A. This is the IP address that's assigned, at least as of, in this case, April 12.
Q. And as a general matter, based on the information you reviewed, was that the IP address assigned to the defendant's computer throughout the events you're going to testify about?
A. Yes, it is.
Q. Let's take a look at an example.
MR. DENTON: If we could go to page 51, Ms. Cooper.
Q. Is that the same IP address that's highlighted here?
A. Yes, it is.

Q. What does this show, Mr. Leedom?
A. So, this is a log file from the ESXi server. This is that server that runs all those virtual machines, and this just shows that the defendant was using that vSphere application to log in to that server to work on. If we go halfway down, we can see this virtual machine named INF_Confluence, that's the Confluence virtual machine.
Q. And what type of user was the defendant logging in as here?
A. If we look at the third line, where it says "local verification as root," like I said before, root is just same word for administrator.
Q. And then down about five lines from the bottom, there's a, next to INF Confluence.VMX, it says "connected to mks-fd," what does that mean?
A. I think for this example, most -- the better line, if we look at the last line, where it says "local connection for mks established," that stands for mouse keyboard screen. So, if you remember from early on in the presentation, there was a picture of what it looks like when you're looking at that server with the virtual machine, and there was that little black box, little play button on it. When you click that and it pops up a window for you to use to navigate the VM and click around, type with your keyboard, that's what this means. It says that box was clicked on, and this mouse-keyboard-screen session was established.

Q. Now, this IP address that's reflected here doing this administrator log-in, that was assigned to the defendant's Windows workstation, is that right?
A. That's correct.
Q. Did the defendant also use other operating systems on his computer?
A. Yes, he did.
Q. How did he do that?
A. So, he had a virtual machine running on his Windows workstation.
Q. And explain a bit about how that works.
A. So, in the same way you'd do it on the server, you can download some software to run a computer inside your computer. It's free. You could go home and do it on your laptop. In this case, he was running a Linux machine on his computer to use for productivity or code or review or programming, things like that.
Q. So when you describe the defendant's workstation, are you referring to a particular computer?
A. Yes.
Q. Which one?
A. So, that's this E0001, like, desktop Windows workstation.
Q. And how is that distinct from his virtual machine?
A. So, kind of hear it called a host, and the virtual machine that's running on that computer would be called a guest. So

kind of call it the host, the host computer.
Q. And do those two computers store information differently?
A. They do.
Q. How?
A. All of the information in that virtual machine that's running on the computer, we kind of treat it as a completely separate, entire computer, like it's -- while it's on the same hard drive, it's all essentially, like, in one big file. So it's just one completely separate piece of information. When it's running, it has a different host name. It has a different IP address. It's like it was just another computer on the network.
Q. And you talked a little bit earlier about log files. Are there separate log files for the defendant's virtual machine and his Windows workstation?
A. Yes.
MR. DENTON: If we could go to the next page, Ms. Cooper.
Q. Did the virtual machine also have a different IP address?
A. Yes, it did.
Q. What was that?
A. You can see it here in the log, second -- I guess third line, "fixed address 10.3.2.35."
Q. And so based on that IP address, are you able to distinguish in some cases between activity that took place with

his Windows workstation and activity that took place with the virtual machine?

A. Absolutely.

Q. Down at the bottom, there's three lines that say renew, rebind, and expire. Do you see those?

A. Yes.

Q. What do those refer to?

A. So, there are a lot of these type of, like, logs that look just like this, except the dates are -- they cover different date ranges at the bottom.

The way computers receive an IP address on a network, it's something called DHCP. It's essentially just a dynamic exchange. So a computer says, hey, I need an IP address, because I don't have one, and you get assigned one. And how long you get to keep that is a specific amount of time. And that's what these last three lines say.

So that just says this IP address, you know, is good until the, you know, expiration date, and it's going to try to, you know, renew it, maybe, for a different one, at this first line, where it says renew. So this is just a simple way of saying on April 20, this is the IP that we can, you know, confirm for sure was this virtual machine.

Q. And to be clear, have you reviewed multiple different iterations of this type of IP address information for the defendant's virtual machine?

A. Yes.
Q. Did the IP address change?
A. No, it did not.
Q. So is this the IP address that we'll see throughout the events that you identified as relevant here?
A. Yes.
Q. Let's talk about some of those events, Mr. Leedom.
MR. DENTON: If we could go to the next slide, Ms. Cooper.
Q. Mr. Leedom, during the course of your analysis, did the period between April 14 and April 18 of 2016 become significant?
A. Yes, it did.
Q. We'll go through in detail, but generally, why?
A. This is when the defendant -- there's some accesses that we'll see for him logging in to certain machines. I believe there was an incident where he changed permissions for a certain project in Stash as well as -- a lot of the admin access to the network was changed over the weekend of the 16th. So this is just an important -- important time frame for us.
Q. Let's start with April 14.
MR. DENTON: If we could go to the next slide, Ms. Cooper.
Q. What conclusions did you draw about relevant events that happened on that day?

A. So, on the 14th, Mr. Schulte used his admin privileges in Stash to give himself permission back to access those OSB libraries. It was just a code repository in Stash.

MR. DENTON: Go to page 55, Ms. Cooper.

Q. First of all, Mr. Leedom, what type of information is reflected here in Government Exhibits 1207-53 and 1207-65?

A. So, these are logs from the Stash server.

Q. And what type of information do they record?

A. Any time a permission was added or removed for a user or a project.

Q. And so what's depicted at the top here?

A. So, this is the time that Jeremy removed Josh Schulte's permissions to the OSB libraries on April 4.

Q. And how do you know that from this exhibit?

A. We won't go through, like, every single one of these lines, but I guess it's easy to see, since it's been kind of redacted and highlighted here. But you can see for both of these two events, at the top, in the black box, we have Jeremy's name. So that's -- it's attributable because you would know who made what changes.

To the left of that, we see "permission revocation requested" event. And then the second line is the actual permission revoked event. That just says hey, we're revoking these permissions.

Want me to just keep going through?

Q. And what permissions in particular were revoked here?
A. Sure. So, if you look in the second line here, it says "permission project admin user Schuljo." So just says we're revoking the project admin permission for Josh Schulte.
Q. And how do you know what project it was?
A. On the very far right, on the first line and the third line, we see OL. That's the internal abbreviation for OSB libraries, OL.
Q. And how are you able to determine the time at which this occurred?
A. Yeah. So, if you look at the very front, there's no -- there's no time stamp. There's an IP address for the user that made the action, but there's no time stamp.

The time stamp in this instance is this long number that's right to the right of Jeremy W. It starts with 145. In technical terms, we call this an epoch timestamp. This is because this is, like, the number of, like, seconds or milliseconds since January 1, 1970. And that's how a lot of computers, especially Linux computers, track time. There's a way to convert this to a normal human-readable time stamp, which if you do that, you'll get that it was on April 4 at 11:21:20 a.m.
Q. And then what's depicted at the bottom here?
A. So, this is the activity from April 14, 2016, when Josh Schulte restored his own administrative permissions to OSB

libraries.

Q. And explain how you know that from Government Exhibit 1207-65.

A. So, we'll look at the first part. This is the IP address that was used. We know this 165 address was Schulte's workstation.

The next piece is, instead of a permission revoked, this is a permission-grant request.

The next line -- or the next piece is the user who's requesting the request. In this case, it's Schuljo. We have a time stamp, which we know resolves to April 14. We have the project that's being actioned, which is again OL, OSB libraries, and then the permission that's changing. So it's a permission grant for project admin to user Schuljo from user Schuljo, essentially granting it to himself.

And then the second line is the actual -- the actual grant event. First line's like, hey, I'm requesting this, and then it was granted. So that's just the log.

Q. And does some person have to take some action to generate the event depicted in the second line there?

A. It's handled, like, by -- as long as the person who requested the permission change has the permissions to make the change, then it's automatic.

Q. So let's turn to the next day, Mr. Leedom.

MR. DENTON: Go to page 56, Ms. Cooper.

Q. What conclusions did you reach about relevant events on April 15, 2016?

A. So, there's two main things that happened. The first thing that happened was Josh attempted to mount that Altabackup share from a, like, different location, that it wasn't able to be mounted from. So we're going to get into that in a second.

The second thing was he used his SSH key, which we talked about earlier, to log in as an administrator to that ESXi virtual machine server.

Q. So let's go through some of the steps that were necessary for that.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. First of all, Mr. Leedom, where is Government Exhibit 1209-9 from?

A. So, this is from a log file from that ESXi server.

Q. And what type of log file?

A. The host D log file. It's a log file that tracks log-ins from that, like, vSphere application on someone's desktop.

Q. Explain to us what the top two lines of this exhibit show.

A. Sure. So, this shows that Josh, where it says user DevLAN/Schuljo from his IP address logged in from that -- when you see VMware-client, that means the vSphere application from his desktop.

Q. And logged in to what?

A. He's logging in to the actual ESXi server, like, the server that runs all the virtual machines.
Q. And are you able to determine from this what time he did that?
A. Yes. It's time stamped on the left here. This is in UTC, with the Z at the end. So we'll have to convert it. But it's April 15, 2016, at about 3:36 p.m.
Q. And then what does the bottom three lines show?
A. So, this is, again, that ticket issued for MKS service log. So clicking on that black box, going into a virtual machine for the Confluence virtual machine, which we can see by that INF_Confluence.
Q. And do you see where, at the end of that line, it says to userdevlan\shuljo?
A. Yes.
Q. How is that different from the user root log-in that we were looking at just a moment ago?
A. So, every user on DevLAN has one of these DevLAN slash username accounts. So this would just mean he's using his, like, normal user account versus the actual, like, administrator account for the ESXi server.
Q. Did this account have administrator access to that server?
A. No.
MR. DENTON: If you could go to page 58, Ms. Cooper.
Q. What did the defendant try and do at 3:47 p.m.?

A. So, without reading through every line here, he attempts to create a data store to that Altabackup share.

Q. And just if you can give us the highlights, what are the relevant pieces of Government Exhibit 1202-7 that tell you that?

A. So, on the first line, we see, you know, "create nas data store." This is just saying that he's essentially creating a, like, a mount point that can be used for that entire server. So, like any machine on that server would be able to use this and, like, go to that backup folder.

Q. Which server was the defendant trying to create this on?

A. This is on the ESXi server, the server that runs all the virtual machines.

Q. And how do you know that?

A. Because we know that these are -- these are VI client logs. So the only thing you log in to with VI client, and especially when you're looking at data stores, host data stores, that's the ESXi server.

Q. So please continue.

A. We just go through this, it's kind of the request.

Drop down to, like, line 5, this is the IP address of the actual file server. This is the path on that file server that we want to mount, that slash Altabackup.

This is -- local path means, like, this is what it would show up as if someone was going to, like, mount it on the

server itself, just show up as backup.

And access mode "read write," and the type is NFS. That's the protocol, the network protocol to use to connect to the server.

Q. How are you able to determine that this was the defendant doing this?

A. So, if we look at the location of where this log came from, this log came from Schulte's workstation, from his VI client logs, which are the logs for that vSphere application. So we know that from looking at the log-ins to Mr. Schulte's workstation, he was the only user that used that workstation, so determine that logs from the client from that workstation are attributable to him.

Q. Was the defendant successfully able to create a data store to the Altabackups?

A. No.

MR. DENTON: Go to the next page, please, Ms. Cooper.

Q. What does this show?

A. So, this just shows that it didn't work. There was an error.

If we go to the line that says message, about two-thirds of the way down -- yeah, that one. This kind of explains why it didn't work. It says the mount request was denied by the server.

What this tells me as an investigator is that, like,

there's access controls on that server for where that data is allowed to be mounted from. There's something called an allow list or a block list that you'd use, specifically with the NFS protocol, where you actually put in specific IP addresses of machines that are allowed to access that server. And, you know, this tells me that since it wasn't able to be mounted by the IP address that that server had, that those restrictions were in place.

Q. Now, just to be clear, Mr. Leedom, were you able to recover the actual allow and block lists for the Altabackups?

A. No.

Q. But were you able to infer this from this exhibit?

A. Yes.

Q. So let's take a look at that in the context of the network overall.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. Explain a little bit about how those permissions affected access to the mount points for the backups.

A. Sure. So, if you were just on a normal computer on the network, with that allow list in place, like, your IP address wouldn't match that of, like, the Confluence VM that's allowed to store stuff in those backups. So you wouldn't be able to go in and mount that share. So the only things that were allowed to access that share were the services that needed access to

it.

Q. And which services were those?

A. I'll say from drawing lines again, but the Confluence, Bamboo, Stash, Crowd, and Jira services.

Q. And when you say services, were the mount points located within the services themselves, or were they located someplace else?

A. So, if the service was running in a virtual machine, the mount point was inside that virtual machine. So that ESXi server itself, like we saw in the previous page, it couldn't mount this. So you'd have to mount it on one of the VMs.

The Stash server, since that's a bare metal server, no VMs, it was mounted directly there.

I'm not sure exactly about this state for Jira and Hickok, but it would be similar.

Q. So moving on from that mount point, what else did you identify that was relevant that the defendant did on April 15, 2016?

MR. DENTON: If we could go to the next page, Ms. Cooper.

A. So, one of the other really important things that happened on this day was the defendant logged in to that ESXi server with his SSH key, and we'll see this session stay open for a while. And it will be -- it will come up throughout the rest of the presentation.

Q. So let's unpack the different pieces of that. First of all, how do you know it was the defendant who did this?

A. So, there's a couple ways that we can tell. I'll just kind of go through each of them.

If you want to highlight the IP address on the first line, we know that this is the IP address for Josh's virtual machine on his workstation, that .35. In the second line -- actually, we'll skip the second line.

On the third line, where it says, you know, accepted public key, this is that public-private key SSH door lock key thing that I was talking about earlier, and at the end of the line here, we see where it says RSA and a bunch of letters and numbers separated by colons, this is essentially the unique identifier or fingerprint for Josh Schulte's key fair. So this essentially says, Yup, this is the key that was used, and the rest of this just says that the session was successfully authenticated for the root user, meaning the admin user.

And the most important thing on this slide, if you could highlight the numbers 11130766 right next to SSHD on the last line.

So, this is called a work ID. When you log in to an ESXi server with an SSH key, and you can run commands on it, your whole session for that log-in is tied to a unique identifier. So no matter how long that session stays open, if it has this identifier next to it, you can determine that this

was the authentication session that was used. So if we see a command run that's tagged with this 11130766 number, we know that that command was being run by Josh Schulte, because we know that the session that was used to connect to the server that got that work ID was used with his private key and came from his computer.

Q. When you were talking about the private key, you referred to a fingerprint. What is the fingerprint in relation to the public and private keys?

A. So, you can essentially take the key fair and run a command and it will just generate this fingerprint. It just lets you determine, you know, what the, what the key is. They get kind of long, so it's just an easy way to quickly know what the key is that's being used.

Q. Let's take a look at that for a second.

MR. DENTON: If you could go to the next page, Ms. Cooper.

Q. What is this, Mr. Leedom?

A. So, this is the public key. So, like I -- my description earlier, let's say you want to put a lock on the courtroom door, this is the lock. So if you want to be able to access the server, you would drop this big blob of text in the right spot on the server, and you can access it.

Q. And where on which server was this public key?

A. So, this is on the ESXi server in a file called authorized

keys.

MR. DENTON: Now, if we could then go to page 63, Ms. Cooper.

Q. I'm not going to ask you to read this, Mr. Leedom. Tell us what we're looking at here.

A. So, this is the private key. So this is the actual key for that lock.

Q. And where did you find this?

A. So, this is on Josh Schulte's virtual machine.

Q. And again, is that the virtual machine on his computer?

A. Yes, that .35 IP address.

Q. And is that distinct from it being on his regular workstation?

A. Yes.

Q. Do you see at the top where it says "4, encrypted"?

A. Yes.

Q. What does that mean?

A. So, let's imagine in our key and lock example, so you have your key. If you wanted to give that key to a friend of yours to also open the lock, you just give him the key, they take your key, open the lock, it works.

Well, what if you wanted it to be more secure? You can put a password on your key. So only someone knowing the password for that key can actually use it. So if you give your friend this key and they don't know the password, they actually can't

use it to open the lock. So it's just another method that we can go to show how we know that it was Josh Schulte who used this key, because he encrypted it with a password.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. What was the password for the defendant's private SSH key?

A. It was KingJosh3000.

Q. Using all of that information that we've looked at on the last three slides, were you able to calculate that key fingerprint?

A. Yes.

MR. DENTON: Let's go to page 65, Ms. Cooper.

Q. And did you compare that with the key fingerprint depicted in Government Exhibit 1209-13?

A. Yes.

Q. Did they match?

A. Yes, it did.

Q. I want to take a look at this from another angle, Mr. Leedom.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. What does this show, Mr. Leedom?

A. So, this is an example of commands that the defendant ran while on that ESXi server.

Q. And so what kind of privileges did the defendant use to run

these commands?
A. So, he had administrator privileges. You can see the very first line of that blocked out, highlighted text, it says root@OSB. OSB is the host name of that ESXi server.
Q. And what is the command that he runs first?
A. Tries to run a command called "last."
Q. Did that work?
A. No, it did not.
Q. Why not?
A. So, that's a Linux command. Unfortunately, that command is not available on the type of Linux that's running on the ESXi server, so that just -- that command wasn't there.
Q. So what command did he run instead?
A. He ran the "who" command. I guess, explain what the "last" command does, it shows you all of the last successful log-ins to the server. So if you wanted to see, you know, who was logged into the server, you run that command. Conversely, the "who" command shows who is currently logged in to the server.
Q. And who was currently logged in to the server at the time the defendant ran this command?
A. So, there's only one, only one session. We can see root. It's the session that ran who. It's the Schulte session. We know it was the first session on the server. That second line that says char/pty/t0 -- that t0, if, like, multiple people started logging in, it would start incrementing to t1, t2.

It's just the virtual terminal that's given to the user that logs in. We have the date that the log-in occurred and the IP address that is, like, using this.

Q. And does that IP address correspond to one of the defendant's computers?

A. Yes.

Q. Which one?

A. It's his virtual machine.

Q. What, if any, conclusions were you able to draw from where you found this record?

A. So, this is from the unallocated space, which I mentioned before, the space where we find, like, evidence -- remnants of deleted files or old files inside of that virtual machine on Mr. Schulte's desktop.

Q. And is the unallocated space for that virtual machine distinct from the unallocated space for his main Windows workstation?

A. Yes, it is.

Q. Let's keep going, Mr. Leedom, and talk about Saturday, April 16, 2016.

MR. DENTON: If we could go to the next slide, Ms. Cooper.

Q. What conclusions did you reach about relevant events that occurred on that day?

A. So, on April 16, this is that -- I think it was a Saturday,

where ISB changed all those admin privileges on the network.
Q. And was that significant in your analysis?
A. Yes, it was.
Q. Why?
A. When you have the network as it existed -- like, before this day, there are multiple different admins that could access different servers. After the 16th, they significantly locked it down and removed, like, all but, you know, like, one account's access from all of these machines. So it significantly reduces the footprint of people who are able to access these -- these computers.
Q. So let's walk through that day. Starting at, with the next page, Ms. Cooper, No. 68, what does this depict, Mr. Leedom?
THE COURT: Mr. Denton, would this be a natural place to stop?
MR. DENTON: Yes, your Honor.
THE COURT: Why don't we do that and pick up on that day when we get back.
Ladies and gentlemen, it's 11:38. You know the drill. Don't discuss the case. Don't communicate with anyone about the case. Don't do any research about the case. Continue to keep an open mind.
Please begin to get ready at 12:15 so we can start promptly at 12 -- ideally, 12:18, but certainly by 12:20, and we'll see you at that time. Enjoy your break. Thank you.

(Jury not present)

THE COURT: You may be seated.

Mr. Leedom, you're welcome to put your mask on and step down. Please be back in the courtroom at 12:15, ready to go.

THE WITNESS: Thank you, sir.

THE COURT: Mr. Denton, I'm assuming that we may not be done with direct by the end of the day. What's the current pace, do you think?

MR. DENTON: I very much hope we will be done with direct by the end of the day. I'm pretty much exactly at the halfway point, but I think it's going to -- it moves pretty quickly from here on out, so I'm optimistic that we'll be able to start cross, but it will be close.

THE COURT: And more broadly, any sense of where we are vis-à-vis your projections? Are we on pace, running behind?

MR. DENTON: I think we're about two full days behind. I think we thought we would be here, you know, Thursday, Friday.

THE COURT: OK. That's unfortunate, but such is life.

I think give some thought to this exhibit. It's not -- I think the problem with it is it's sort of a hybrid of a 1006 exhibit, which would be admissible, versus a demonstrative, which wouldn't be. I think for that reason I'm

not inclined to admit the entirety of it as an exhibit, but I don't know how you want to handle that, if you want to admit portions of that or label them separately as 1703 dash something, but why don't you give that some thought and we can discuss it later. It also may be that you don't need it as an exhibit to go into the jury room, but you should give it some thought to discuss later.

MR. DENTON: Understood, your Honor.

THE COURT: And you'll give me a copy of the older version so that I can compare?

MR. DENTON: Yes, your Honor.

THE COURT: Anything else for you to discuss?

MR. DENTON: Not at this time, your Honor. No.

THE COURT: Mr. Schulte.

MR. SCHULTE: Just a couple quick things.

First, I just wanted to let the Court know that in the new 1703, specifically pages one -- slides 118, 119, and 130 are the new ones. And then I want to note that depending on how the government, once they get a chance to look at the letter that I sent them, there may be a need to introduce the classified exhibit that's been admitted, another classified I mean, and potentially issues with other exhibits on cross.

THE COURT: All right. Well, that's not happening this afternoon.

Has the government received Mr. Schulte's letter?

MR. DENTON: No, your Honor.

THE COURT: How has it been --

MR. SCHULTE: It's on the CD that I gave. I couldn't print it, so it's just on the CD.

THE COURT: Why don't you take a look at that. To the extent we need to discuss it, we'll discuss it at the end of the trial day and go from there.

All right. I will see you at the break. Please be here 12:15, no later, and we'll get ready to go promptly thereafter.

Thanks.

(Luncheon recess)

A F T E R N O O N S E S S I O N

12:15 p.m.

THE COURT: We will get the jury in a second unless there is anything to discuss.

I did review the 2020 version of Mr. Leedom's presentation and the current one. As far as I can tell, the content on the pages Mr. Schulte pointed to -- 118, 119 and 130 does, indeed, appear in the older version, albeit not necessarily broken out in the same way.

Is that correct, Mr. Denton?

MR. DENTON: Yes, your Honor.

THE COURT: Anything else to raise while I look for that?

MR. DENTON: Not from us, your Honor.

THE COURT: Mr. Denton, do you by chance have handy the pages that they correspond to?

MR. DENTON: I left the post-it note downstairs, your Honor. I think it is 163 through 165, if I remember correctly.

THE COURT: I have pages 132 and 133 I think include all of the same content that appear on 118 and 119 in the current version. That is to say that it says the defendant deletes log files of his activities 5:55 to 5:57 and appears to be a list of the relevant log files -- again, they're broken out individually in the current version but the content is the same. And then, 130 appears to correspond to page 148 in the

old version, again the content being the same, presentation slightly different. So on the basis of that, I think there is no merit to Mr. Schulte's concern and we will proceed. We will get the jury and continue.

While we are waiting, Mr. Denton, I don't want to discuss the substance now but have you seen a copy of Mr. Schulte's letter that he alluded to?

MR. DENTON: I have physically seen it printed out. I have only had a chance to skim it, your Honor.

THE COURT: That intended just as a letter to the government or should I also have a copy of it?

MR. DENTON: I believe it was just addressed to the government, your Honor.

THE COURT: OK. Then I won't ask for a copy.

THE DEPUTY CLERK: Jury entering.

(Continued on next page)

(Jury present)

THE COURT: You may be seated. Welcome back. I hope you enjoyed your break. We will pick up where we left off with the direct testimony of Mr. Leedom.

Mr. Leedom, you may remove your mask at this time and I remind you, you remain under oath.

THE WITNESS: Yes, sir.

THE COURT: Mr. Denton, you may proceed.

MR. DENTON: Thank you, your Honor.

BY MR. DENTON:

Q. Mr. Leedom, just briefly before we pick up with April 16th, 2016, when you testified on Friday, you testified about having been an employee of the MITRE Corporation; is that right?

A. Yes.

Q. When you were conducting all of the work you were testifying about today were you a MITRE employee?

A. Yes, I was.

Q. Were you working specifically on this case or were you a MITRE employee more generally?

A. I was a MITRE employee generally.

Q. And was your work with the FBI unique to this case or were you supporting the FBI more generally?

A. I was supporting the FBI in the same way we supported all the cases.

Q. Do you know whether MITRE's contract with the FBI that

provided for your services in any way depended on this case in particular?

A. No.

MR. SCHULTE: Objection.

THE COURT: Overruled.

Q. I believe you testified you no longer are a full-time employee at MITRE; is that right?

A. That's correct.

Q. Do you still have a relationship with MITRE in connection with this case?

A. Yes, I do.

Q. What is that?

A. To contribute and prep for the session here.

I had to have clearance, and when I left MITRE to work for Microsoft they only held a portion of my clearance. There is a bunch of extra compartments and things that go with that that go with data on this case, so to have access to the facilities needed to review and, like, update things like the presentation I had to have clearance on file. So the best way that the government decided to do that was to just have me go back on as an independent contractor for MITRE to re-hold my clearance through the bureau like it was before.

Q. And are you being paid for your work specifically on this case now?

A. Yes.

Q. What work are you being paid for?
A. So it is just the work related to the trial, prep, like travel arrangements. Things like that.
Q. And who is paying you for your substantive work?
A. It comes from our, like, the MITRE contract with the FBI, it is just like a chunk of money was blocked off to do that.
Q. Is the U.S. Attorney's office paying for your travel expenses up here?
A. Some of the lodging expenses, yes.
Q. Is your compensation in any way tied to the conclusions that you express in court today?
A. Not at all.
Q. Let's turn back to Saturday, April 16, Mr. Leedom. Just to remind us, overall, what were the significant events that you identified as occurring on April 16, 2016?
A. April 16 is when ISB changed all of those admin passwords to those servers.
Q. What was the first relevant event that you identified on April 16th?
A. This was changing the password for the Confluence virtual machine specifically creating a snapshot for that machine.
Q. Explain to us what is depicted here on page 68 of Government Exhibit 1703.
A. So this is a log from the actual -- there is a log file for the Confluence virtual machine that keeps track of everything

that happens to the virtual machine. This is that log file and this is a piece of it that shows the snapshots for that virtual machine. Specifically, on April 16th, we are going to be looking at snapshot 2. This snapshot was created on the 16th before ISB made any changes to the admin passwords.

Q. How are you able to tell when these different snapshots were created?

A. So if you look in the red box portion, right in the middle you have that createtimehigh, and low. That's just the way it logs this. You can convert it into something that is readable which is actually readable over here on the right and you can see that was 4/16/2016 and 1:42 p.m.

Q. Does that require using a computer program of some kind?

A. You can Google createtimehigh low and there will be a script that you can pull down and it will convert it for you.

Q. How many snapshots are depicted here, Mr. Leedom?

A. Right here on this page there is three snapshots.

Q. It looks like we have snapshot 1, snapshot 2, and snapshot 4; is that right?

A. That's correct.

Q. What, if any conclusions, did you draw about the fact that there is no snapshot 3?

A. It was deleted at some point.

Q. Were you able to examine this April 16th, 2016 snapshot of Confluence?

A. Yes.
Q. And what name was assigned to that snapshot?
A. It's the fourth line in the red box, it says Display Name bkup 4-16-2016.
MR. DENTON: So if we can go to the next page, Ms. Cooper?
Q. From that April 16, 2016 snapshot, which SSH keys could be used to access the Confluence virtual machine?
A. So there were quite a few. We have listed them here. There is -- it looks like seven -- seven keys.
Q. And which key is at the top there?
A. This is the defendant's public key.
Q. Is that the same one we were looking at earlier?
A. Yes, it is.
MR. DENTON: So then if we could go to the next page, Ms. Cooper?
Q. After those changes were made, how many authorized keys could access the Confluence virtual machine?
A. Just one.
Q. Was it the same as any of the previous keys?
A. Nope. It was a new one.
Q. What effect, if any, did that change have on Mr. Schulte's ability to access the Confluence virtual machine?
A. He would have been unable to access it.
MR. DENTON: Go to the next page, Ms. Cooper.

Q. In addition to the changes to the SSH keys, were there also changes to passwords made on that day?
A. Yes.
Q. How were you able to determine that?
A. So the password on a computer is stored as essentially this big string of obfuscated numbers and letters. It would be bad to store, like, the plain text password, if someone came across it then they would have it. So the computer does this to store it in a way that is usable by the computer and also obfuscated. So basically we can take a look at the file where this -- we call it a hash is stored, and look at two different dates and we can see that it's changed.
Q. Is that what is depicted here in Government's Exhibits 1207-11 and 21?
A. Yes.
Q. Without asking you to read the whole thing, are those passwords different?
A. Yes, they are.
Q. In addition to changes to the Confluence virtual machine, were you able to determine if any other changes of significance were made on April 16th, 2016?
A. Yes.
MR. DENTON: Go to the next page please, Ms. Cooper?
Q. What other change was made on April 16, 2016?
A. So the password for that ESXi server was also changed.

Q. So explain to us what we are looking at, both in general and then in the red box on this slide.
A. So this is similar to that log file we looked at before.
MR. DENTON: If you could highlight the fifth row, the session open row? Perfect.
A. So this is where we ended this snippet the last time we looked at it. We talked about the work ID ending in 766 so this is the same log file I think going to the end of it to show some future dates. So starting with this 15th activity, this is when Josh logs into the ESXi server with his private key, and then if we go down to the 16th we can see another session where someone is logging into the server and changing the password for the root account. I think there is only one real account on that computer, it is the root admin account. So, he logged in using user name and password and changed the password.
Q. And do you know who made that change?
A. Yes.
Q. Who did that?
A. I believe it was Jeremy.
Q. How do you know that?
A. On the first line in the red box towards the end there is an IP address and we determined that that is his IP address. I think it also shows up in the log for the OSB library changes as well.

Q. Were you able to verify that that password for the OSB ESXi account had also in fact been changed?
A. Yes.
MR. DENTON: Can we take a look at page 73, Ms. Cooper?
Q. Is this the same type of password information like we were looking at for the Confluence virtual machine a minute ago?
A. Yes, it is.
Q. But for which computer is this?
A. This is for the ESXi server.
Q. And again, without asking you to read all of these letters, are they different?
A. Yes, they are.
Q. Now, in the content of the Confluence virtual machine we talked about changes to both passwords and SSH keys; is that right?
A. Yes.
Q. Were both of them changed on the Confluence virtual machine on April 16, 2016?
A. Yes, they were.
MR. DENTON: Let's go to the next page, Ms. Cooper.
Q. What about on the OSB ESXi server, were both passwords and SSH keys changed on April 16, 2016?
A. They were not.
Q. What does page 74 show here?

A. So this shows the same, like, authorized keys file which has, like, all the keys -- the public keys that are allowed to be used to log into the server and after April 16th, Josh Schulte's key was still available on that server.

Q. I want to talk about how these different administrative changes kind of interact with one another. If we could go to page 75, Ms. Cooper?

First, Mr. Leedom, what is the significance of the fact that this snapshot of the Confluence virtual machine bkup 4/16 was created?

A. So since they made this backup that had the different credentials stored in it, if you were to revert the Confluence machine at any later date to that backup you would be able to log in with whatever passwords were in play at the time.

Q. And so what other changes then happened to the Confluence virtual machine?

A. So after they created the backup they went and replaced all of the SSH keys with a new one and then changed the administrative password.

Q. And just to be clear, are those changes reflected in that bkup 4-16 snapshot?

A. No.

Q. What effect did those changes have on the defendant's ability to access the Confluence virtual machine?

A. They completely removed his ability to log in and access

that server.
Q. What about the ESXi server, what effect did the changes reflected there have?
A. So the administrative passwords changed -- I guess if it wasn't clear before there is two ways you can log into the ESXi server, you can use a user name and password or you could use your SSH key to do it. So in this case they just changed the user name -- well, they just changed the password, the user name was the same, but they didn't remove the SSH key. I can explain why, if you want.
Q. Let me ask, first of all, are the logins between password and SSH key essentially the same?
A. It gives you the same level of access. They are, like, logged differently in the log file but the access you are granted is administrator access.
Q. And so you were going to explain about the SSH key in a moment.
A. Yes.

So the reason it was -- I will say the likely reason it was missed is on ESXi, since it is a different version of Linux, the location that this file is stored at is actually a little bit different than on normal -- like normal Linux computers. So even if you are an admin for those types of environments, it's in a different place, you have to know where to look for it so I guess that's why it was missed.

Q. So what effect did the changes to the ESXi server have on the defendant's ability to access it as an administrator?
A. Essentially no effect.
Q. As an administrator to the ESXi server, would the defendant have been able to do anything with respect to the Confluence virtual machine after April 16, 2016?
A. Oh yes.
Q. Like what?
A. He would have full access to all of the, like, controls for the virtual machine so you could delete it, you could turn it on, turn it off, you could revert it to another snapshot, you could make new snapshots, whatever you want to do on the server.
Q. Would he have been able to log into the virtual machine?
A. No, not in the state it was in after the passwords were changed.
MR. DENTON: If we can go to the next page please, Ms. Cooper?
Q. Did you also identify relevant events that occurred on April 18, 2016?
A. Yes.
Q. We will go through those in a little bit of detail.
MR. DENTON: We can go to the next page, Ms. Cooper?
Q. What does this show, Mr. Leedom?
A. So this is a failed login to the Confluence VM from

Mr. Schulte on April 18 at 11:08.
Q. Now, when you say from Mr. Schulte, which of the defendant's computers was he using to attempt to log to the Confluence virtual machine?
A. So this is from his virtual machine on his desktop. We know that because the IP address is listed a couple times here, the .35.
Q. And then you have two different types of logins listed here. How are you able to tell the difference?
A. So we can see there is both a, like a pam -- so if we look at the first three lines about in the middle there is an SSHD and then a number that's like the type of service. So, SSH is that public private key thing we have been talking about so that was like an attempt to use that key. And then, underneath it here with login where it says pam_UNIX, this is like user name/password.
Q. And were those login attempts successful?
A. No.
Q. How do you know that?
A. We can see in the first case the connection closed and in the second case we have a failed login.
Q. And I think you said these were attempts to log directly into the Confluence virtual machine; is that right?
A. That's correct.
Q. Let's take a look at the next slide. Was the defendant

successful logging in anywhere on that morning?
A. Yes.
Q. Where?
A. To the ESXi server.
Q. So explain a little bit about what we are looking at here.
A. So in the top here we have a login -- so these are both log files from that server, and like we have seen before from the VMware client, so this is from that vSphere application on his desktop. In the far right of the first line we see user root@ the next address, the 10.3.2.165 so Mr. Schulte's windows desktop logging in to the ESXi server.
Q. And then what does the entry underneath that show?
A. So this --
Q. Let me be clear. The two lines that are also highlighted in black below what you were just reading from Government Exhibit 1209-17?
A. Yes. So this is showing what virtual machine he has selected on the server, in this case the INF_Confluence virtual machine. And like we have seen before, the ticket issues for MKS service so clicked on the black box, tried to access it.
Q. And what type of user was doing that?
A. So he is the root user for the ESXi server.
Q. And what kind of privileges did he have as the root user?
A. Administrative privileges.
Q. Do you see an entry below that for DevLAN/Matt?

A. Yes.
Q. How is that different than the entry for the defendant's login?
A. So where it says user equals DevLAN/matt, that's a normal user count for DevLAN. I think we saw earlier Mr. Schulte logged in using his normal user account at one point and it said DevLAN/SchulJo, so that is difference between logging in with non-administrative account versus the root account which is the administrative account.
Q. And did this session that the defendant logged into at 11:12:09 eventually end?
A. Yes.
Q. How do you know that?
A. We have a logout log for it.
Q. Is that what's depicted in Government Exhibit 1209-20?
A. Yes, it is.
Q. What time did that session end?
A. At 1:47:49 on 4/18.
Q. And are these times that you are describing from the actual timestamps in the log file?
A. They're converted. The timestamps in the log file, you will see the Z, those are UTC times so converted them to Eastern Daylight Time to make everything consistent.
Q. I think you said, Mr. Leedom, that this administrator login to the ESXi server was from the defendant's windows work

station; is that right?
A. Yes. That's correct.
Q. Was he also logged in from his Linux virtual machine at the same time?
A. Yes.
MR. DENTON: Go to the next page please, no. 79, please, Ms. Cooper?
Q. How do you know that on April 18 the defendant was logged in from his virtual machine as well?
A. So this is pretty important as we look through the logs on the ESXi server but do you see how all of this activity on the 16th and 18th there is the last four lines of this log, the first of those we had like -- sorry, the second to last one we had session closed. So when a user connects there will be an event for them creating the connection and then an event for them closing the connection when they leave. We don't actually ever have a connection closed for that work ID 766 that we discussed earlier for the defendant's connection on the 15th. So what does that mean? It just means when he logged in on the 15th, that connection stayed open over the weekend and into the next week.
Q. And did you identify activity using that work ID after April 18th?
A. Yes.
Q. And so what does that indicate about the state of that

session on April 18th?
A. It was clearly open since commands are being run from that work ID.
MR. DENTON: If we can go to page 80, please, Ms. Cooper?
Q. Mr. Leedom, what's the date and time of this e-mail?
A. This is on April 18th, at 12:59 Eastern Daylight Time.
Q. And who sent it?
A. This is from Josh.
Q. If we can go to the next page, please, Ms. Cooper?
Do you see the line that says: All private keys with access have been destroyed/revoked?
A. Yes.
Q. At the time this e-mail was sent, was the defendant using any of his private keys?
A. Yes, he was.
Q. Which ones?
A. He was using the key to access the ESXi server when he logged in on the 15th.
Q. And a little further down where it says: It seemed like overnight literally all my permissions within the products were removed and all my permissions on the servers themselves were revoked.
Was the defendant accessing any servers at the time this e-mail was sent?

A. Yes, he was.
Q. Which ones?
A. The ESXi server.
Q. Was he attempting to do anything with respect to the Confluence virtual machine at that time?
A. He had, like, attempted to log into it on the 18th.
Q. Now, just to turn to a little bit later in that day on April 18th, did you identify any other activity of the defendant on that evening?
A. Yes.
MR. DENTON: Go to page 82, Ms. Cooper?
Q. Before we get into the specifics, at a general level, Mr. Leedom, what was the type of activity that you identified on April 18th?
A. He was on the -- again, on the ESXi server. We know it is his session because we have this 766 work ID, and without going through all these commands, this is just him listing log files and viewing log files on the server on the evening of the 18th.
Q. And where was this file, Government Exhibit 1203-43, found?
A. This was found on Mr. Schulte's desktop work station in the virtual machine on his desktop.
Q. And again, when you say in the virtual machine on his desktop, is the place where this was found distinct from his Windows work station?
A. Yes, it was.

Q. And what, if any significance, do you attribute to the fact that this was found in unallocated space?
A. It just means at some point the files containing this data were deleted or otherwise like -- yeah, deleted.
Q. And were you able to tell specifically how or when they were deleted?
A. No.
Q. But is it fair to say that at some point they were deleted?
A. Yes.
Q. What do the letters "ls" at the start of the black highlighting identify?
A. That's a command that you would type in, it stands for list, show me all the files in this folder, pretty much.
Q. And then there is a version below that, ls -al. What is the difference there?
A. We call the -al, like, arguments. So al means show all files, this will include like hidden files, you can have hidden files on Linux, and the "L" is like show it to me like in a column list format -- so it makes it easier to read.
Q. What's the time of these entries, Mr. Leedom?
A. This is April 18th -- the evening of April 18th.
Q. Approximately what time?
A. Let's see. So that's 10:00, so like 6:08 p.m.
Q. Let's look at a little bit later that evening.
MR. DENTON: If we could go to page 83, Ms. Cooper?

Q. First of all, Mr. Leedom, again, where does this file come from?
A. So this comes from the ESXi server.
Q. And what does it show?
A. So this is the same I think we were looking at from before but this time on the server side. These are just commands that were run by the defendant.
Q. And how do you know they were run by the defendant?
A. Because all these commands are attributed to that 766 work ID.
Q. Just to take a couple of examples here is there any significance to you to the type of commands that the defendant is running?
A. Yes.
Q. What is that?
A. So just kind of summarize this as we are looking at it. He is basically going through, looking at log files, looking at some -- when we see the middle here, we see vi, vpxa.log, vi is a command to view or edit a file so it will let you go into it and look around and you can edit it and save it and close it if you want. And the rest of the stuff after this, to just kind of summarize it, he is unzipping some older log files and looking at those as well.
Q. To take another example of something we looked at before, Mr. Leedom -- if we could go to page 84 -- is this another

comparison of that version we looked at earlier?
A. Yes, it is.
Q. Again, what is the difference between what is recorded in Government Exhibit 1209-8 and what is recorded in Government Exhibit 1203-44?
A. So normally when you are looking at logs from a server like this it just shows you the command that was run, so in this case ls -al command. It is pretty rare that there is no log files on the server that show the output from the command. As you could imagine, that would be like a lot of space. So this bottom entry here, since we have Mr. Schulte's virtual machine where he was running these commands from and actually, like, viewing it on his screen, we have the output from that command. So when he runs this ls -al command for this log directly we can actually see what the output from that command was. So this is essentially what he was seeing when he ran this command.
Q. And what does that total 28271 indicate?
A. So when you run the list command, once you add that "A" flag to give you some more information, this is essentially like a very rough estimate of the size of all the files that it is showing you as a result. It's the number of, like, 512-byte blocks that these files all occupy. So like we discussed earlier with the shoe box, all these files may not fully fill the shoe box so it is a rough estimate but if files are added

or deleted, this number will change.

MR. DENTON: If we can go to page 85, Ms. Cooper?

Q. Is this more from April 18th?

A. Yes, it is.

Q. Is it after the log files that we were just looking at?

A. Yes.

Q. What is the top command there, CD INF Confluence?

A. CD stands for change directly so changing to the Confluence directory.

Q. And what is in that directly?

A. So this is where all the data for that Confluence virtual machine is stored.

Q. And at the time that the defendant was doing this, was he an administrator for that virtual machine?

A. No, he was not.

Q. What are some of the commands that he runs in that directory?

A. He is listing the files to be the files going to the, like, the log directory, to view those, and then inside there he is -- I should say that once he goes up -- let me go to this fourth line here, if we can highlight the CD/scratch? So when he does this he is no longer inside the Confluence VM anymore, he is on the actual ESXi server itself, and then he goes into the log file folder for, like, all the logs for the whole ESXi server and at the very bottom we see a vi shell.log. So if you

look at the bottom of this slide, everything we are looking at here comes from the shell.log file. So he ran the command that lets you edit files to edit the log files that stores the commands that have been run on the server and in this case he removes lines from that file.

Q. So let's take that step by step. First of all, what is vi shell.log?

A. Like I said before, this is the command you use to get, like, a visual editor in the terminal window to either read or make edits to files.

Q. And what is recorded in the shell.log file?

A. All the commands that are run on the ESXi server.

Q. Now, I think the exhibits that we have been looking at for the last couple of pages come from what is listed below here shell.log fileslack; is that right?

A. Yes.

Q. Was there an actual shell.log log file that you reviewed?

A. Yes, there was.

Q. Do these commands that assigned to this work ID appear in that log file?

A. No, they do not.

Q. What, if any conclusions, were you able to reach based on that fact?

A. It is clear that the defendant ran a bunch of commands on the server and then went and edited the log file that logged

his activity to remove any traces of him running those commands.

Q. Now, Mr. Leedom, I want to finally shift to the last part of your presentation and focus on April 20th, 2016.

MR. DENTON: Going to the next page, Ms. Cooper?

Q. Did you identify any significant events on April 20th, 2016?

A. Yes, I did.

Q. Broadly speaking, what were they?

A. So on the 20th, Mr. Schulte accessed that Confluence virtual machine that we have been talking about. He then used the vSphere client to revert it to that 4-16 snapshot from before ISB had changed all of those passwords. It stayed in that reverted state for a little over an hour, in which time Mr. Schulte copied that March 3rd backup from Confluence, those database backups. And then, after that, he was using that session that he opened on the 15th to the ESXi server with his private key that was left and not changed, and he deleted not just the content from that shell.log file but many other log files as well on the ESXi server. And then, kind of to wrap it up, he had created a new snapshot for the Confluence VM before he got started with this process and then restored its state to that new snapshot and then deleted it, which essentially, like, erased any activity that would have happened inside that Confluence virtual machine.

Q. So let's go through this in chronological order, Mr. Leedom.

MR. DENTON: If you can go to page 87? Ms. Cooper if I can ask you to blow up the top two paragraphs here? And if you can move that down on the page, Ms. Cooper? Thank you.

Q. Mr. Leedom, what time was this e-mail sent?

A. This was sent on April 20th, 2016, at 3:58 Eastern Daylight Time.

Q. Do you see where it says: The Atlassian suite (in particular the Bamboo and Confluence servers) will be unavailable, and then ISB will be transferring the data to new servers/hardware.

A. Yes.

Q. Were you able to determine any significance to those planned changes?

A. Yes. So this means that after the 25th of April, those virtual machines running those services would no longer be on that ESXi server, so by the 25th of April the defendant would no longer have access to those services because they would be managed by ISB.

MR. DENTON: If you can go to page 88, Ms. Cooper?

Q. Again, when there is a reference to the server that Confluence and Bamboo are running on, which server was that?

A. It is the server on the top left that is labeled ESXi server.

Q. As of April 20th, what kind of access did the defendant have to the ESXi server?
A. Since his public key was still on there, he had administrative access to that server.
Q. And did he have administrative access to the Confluence virtual machine?
A. No.
Q. What, if anything, did his administrative access to the ESXi server allow him to do to the Confluence virtual machine?
A. So he couldn't log into the Confluence virtual machine since all those permissions are kind of managed inside of it, but since he had admin access to the server that was running it and the snapshots that were made of it, he could revert it to any earlier point in time. In this case the 4-16 backup before the passwords had been changed and then he could access it.
Q. As an administrator of the ESXi server, did the defendant have direct access to that Altabackup mount point that we spoke about before?
A. Not from the ESXi server.
Q. Why not?
A. We saw an earlier example where he actually tried to mount it to that server and it failed.
MR. DENTON: Let's go to the next slide, please, Ms. Cooper?
Q. Starting with the top bullet, Mr. Leedom, why were

administrative privileges necessary to revert the Confluence virtual machine?

A. I guess it was how it was configured to be able to make those -- it is a pretty significant change. It is a big change to the virtual machine, so.

Q. During that time period was there any relevant activity with respect to that March 3rd backup that you talked about?

A. Yes; on April 20th.

Q. Yes. What was that?

A. We saw the access time for those files on the backup share. The last time they were accessed was this time on April 20th.

Q. And then you talked a moment ago about the deletion of log files. Do you remember that?

A. Yes.

Q. Is that normal activity for a server administrator to perform?

A. Not in the way he deleted them, no.

MR. SCHULTE: Objection.

THE COURT: Can you explain the basis for that testimony?

THE WITNESS: Oh. Of course.

So normal -- I will just kind of explain what a normal system administrator does on a computer or a server. So with respect to log files, they're logging stuff all the time so all day, every day, everything that's happening on these servers is

getting logged. An instance where you would delete log files is when you run out of space. Some of these log files get huge. I think we saw an example where the defendant was actually unzipping some of those older log files, they kind of automatically roll over and it will number it. So at some point if you are running out of space you can go and an admin would go and delete older log files because you really only need the last 30, 90 days or so to troubleshoot most issues. So that would be a normal instance.

BY MR. DENTON:

Q. Let me stop you right there. Why would you generally only need the most recent 30, 60, 90 days?

A. Usually, like most user problems that people run into, if someone can't access something to do their job, they're going to come banging down your door to fix it. So usually people don't wait that long to say something is broken but I think, on the whole, that's about the average retention. Stuff could be longer or shorter, especially for log files that aren't written too very frequently, it can cover since the machine was first built they could be around. But for log files, they get big. The only real reasonable reason you would delete them is because you run out of space.

Q. What was different about the defendant's log file deletions that evening?

A. So when the defendant deleted log files he didn't delete

the oldest files first, he actually went and looked for the newest files. Specifically, he went and looked at that, the shell.log file that logs the commands that are entered and actually lists all the log files that had been modified, you know, around the same time that that file had. And he doesn't delete all the log files or parts of the old ones, he goes and deletes all the ones that had changed recently. And as an incident responder having worked on many, like, criminal cases and other cases where people have hacked into a server or do something --

MR. SCHULTE: Objection.

(Continued on next page)

THE COURT: Overruled.

A. When someone has, like, hacked into a server and done something nefarious, and then what they do before they leave is they clean up after themselves. And it looks just like the slides I'm going to show you here. You delete the places where it stores the data that you might've changed. You delete the commands that you entered so that no one can see, you know, what happened. So that's kind of the big distinction for the activities that the defendant did here compared to what would be considered, like, normal admin activities.

Q. So let's take a look at this on a time line, Mr. Leedom.

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

Q. For approximately how long was the Confluence virtual machine reverted to the BKUP 4-16-2016 snapshot?

A. It was a little over an hour. So we've got between 5:35 and 6:51, so, like, an hour and 20 minutes, almost.

Q. Before that reversion, would the defendant have been able to access the Altabackups file?

A. No.

Q. After that reversion, was the defendant able to access the Altabackups file?

A. Yes.

Q. How?

A. Through the Confluence virtual machine.

Q. Was that period of time long enough to copy a backup copy

of Confluence?
A. Yes.
Q. What about a backup copy of Stash?
A. It would have been long enough to copy a backup copy of Stash.
Q. So let's talk about some of these things in particular.
MR. DENTON: If we could go to page 91, Ms. Cooper.
Q. Let's start that evening at 5:29 p.m. What was the first kind of relevant thing that you identified the defendant doing on the evening of April 20?
A. He runs a command on the ESXi server to, like, list files.
Q. And as what kind of user was the defendant accessing the ESXi server?
A. The root user or the administrative user.
Q. And how do you know this is the defendant?
A. From this work ID, this 77 -- excuse me, 766 work ID that we've been looking at.
Q. Now, there's a time stamp on this command, is that right, Mr. Leedom?
A. Yes.
MR. DENTON: If we could then go to page 92, Ms. Cooper.
Q. Does this show that same command?
A. Yes, I believe it does.
Q. And what is the total that's listed there?

A. 28030.
Q. And that refers to the total size of the files, is that right?
A. Yup, it's a rough, rough estimate of the size of every file in this directory.
Q. And which directory is this?
A. This is the logs directory for the ESXi server.
Q. And what, if any, significance is there to the letters ALTR depicted on that second line there?
A. So, you've seen some list commands earlier. We saw the LS-AL, which was list all files in a list like this. The T says sort them by time, and the R says reverse the time sort. So this essentially says sort them by oldest to newest.
Q. Now, in this version of this command, Mr. Leedom, there doesn't appear to be a time stamp, is that right?
A. That's correct.
Q. Is there still a way you're able to approximate what time this command is run?
A. Yes.
MR. DENTON: Go to the next slide, Ms. Cooper.
Q. What are we looking at here, Mr. Leedom?
A. So, this is the bottom of that command. So since we're sorting in, like, oldest to newest, when you're typing on the terminal, everything's kind of like scrolling upwards, so if it's going to, you know, some of the stuff takes up a lot of

space. Your window's only so big. So, like, the last few lines you'll see are going to be the newest files. So that's why you sort it; it's just easier to see it. So these last few are just the last entries from that LS command.

Q. How does that allow you to determine approximately the time that the command was run?

A. So, like I was saying before about the log files, so some of these log files -- and I've independently verified this too -- they're written to, like, every second. So VPXA gets written to very, very frequently. So this date/time stamp here that we see, this is the modified time for that file. And like I'd mentioned earlier, when you make a change to a file, the modified time changes. So we can use these log files to kind of estimate that.

In this case, the shell.log file is also there. So I said the shell.log file stores a log of the commands that are run. So when you run a command, it updates that file with the command that you ran. So naturally, like, if you only ran one command and it's a list command, the file time stamp that shows up for shell.log is going to be the time that that shell.log was written to, which would be right about when you ran the command.

Q. And based on this, what time are you able to approximate for this command?

A. So, it's April 20 at -- like I said, this is UTC. So we

got to convert it. So this is April 20 at 5:29 p.m.

MR. DENTON: If we could go just run back to page 91, Ms. Cooper.

Q. How does that compare to the version of this command recorded in Government Exhibit 1203-2?

A. It's the same down to the minute. We have a little more fidelity on the seconds here, but --

MR. DENTON: If we could then skip ahead to page 94, Ms. Cooper.

Q. I want to start, Mr. Leedom, with the boxes that were in white on the top of your time line that talked about Confluence reversions.

A. OK.

MR. DENTON: If we could go to page 95, Ms. Cooper.

Q. What was the first thing that you identified that the defendant did with respect to snapshots of the Confluence virtual machine?

A. So, in his, like, little vSphere application on his workstation, he viewed the list of all the snapshots.

Q. And how are you able to tell for which virtual machine these are the snapshots?

A. Let's see here.

OK. So, this is a little weird. If we highlight where it says virtual machine snapshot:57, it's in the red box. So 57 is the internal ID number for the Confluence virtual

machine. Sometimes it references it by that ID number. Sometimes it gives the full name, like INF_confluence, but 57 is that, like, ID.

Q. And this particular snapshot, snapshot 2, that's highlighted in red here, is that a significant one to you?

A. Yes.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. Which snapshot is snapshot 2?

A. So, the white box on the bottom is the same exhibit we showed earlier that has the -- this was the snapshot that ISB made right before they changed all the admin passwords.

Q. Did the defendant revert to that snapshot right away?

A. Pretty soon after, after going through the snapshots. He had to create a new one first, but eventually, yes.

Q. Let's talk about that.

MR. DENTON: If we could go to page 97, Ms. Cooper.

Q. What is depicted here, Mr. Leedom?

A. So, similarly, on that vSphere application on the defendant's desktop, he creates a new snapshot at current time, so at, you know, on April 20 at 5:29. So current running time, he makes a new -- a new snapshot called BKUP.

Q. And how do you know the defendant did that?

A. So, if we look -- so, this exhibit comes from the client log from Mr. Schulte's workstation, meaning that the client on

his workstation was used to do this.
Q. What time did he create the snapshot named BKUP?
A. So, we can use the last line of this log for when the snapshot was finished creating. So it's at 5:29 p.m. on April 20.
Q. So let's take a look at where we are on the time line.
MR. DENTON: If we could go to page 98, Ms. Cooper.
Q. As of that time, Mr. Leedom, did the defendant have administrative access to the Confluence virtual machine?
A. Not yet.
MR. DENTON: If we could go to the next page.
Q. About how long does it take to create a snapshot?
A. It depends on how large the virtual machine is and, like, how many changes there have been since the last snapshot was taken. It kind of stores everything. It's like a delta. Like, it says, here's all the changes that have happened since, you know, the last time we did this. So it's been a couple days, so the changes are going to be somewhat minimal so that it doesn't take too long to make the snapshot.
Q. And what are we looking at here?
A. These are logs for the Confluence virtual machine. I think this is like kernel logs from the ESXi server. It's kind of who the -- it's kind of difficult to explain because these log files have been deleted, so you can't actually see these right now. The only way you're able to recover them was from

Mr. Schulte's virtual machine. So this is, like, the kernel log from the ESXi server showing what was happening to that Confluence VM when Mr. Schulte made the backup.

And just to answer your previous question about how long did it take, we can just look from the first to the last. It was -- what is that? 20 -- I'm sorry. 40 -- like 40 seconds or so.

Q. And again, just taking the top and bottom lines that are highlighted in black here, what is this Government Exhibit 1203-25 depicting?

A. This is showing that the defendant, you know, went to create a new backup called BKUP, and that backup was successfully created.

MR. DENTON: Let's go to slide 100.

Q. Walk us through what this depicts, Mr. Leedom.

A. So, this is from Mr. Schulte's workstation. So this is from the vSphere application, and the first thing that happens is this is showing that a pop-up dialogue popped up, like a warning, that said, hey, the current state of the virtual machine will be lost unless you've save it in this snapshot. Revert to snapshot BKUP 4-16-2016. So this is Mr. Schulte reverting that virtual machine to the 4/16 snapshot that ISB made that had the old admin passwords.

MR. DENTON: Could we go to the next page, Ms. Cooper.

Q. So walk us through the top and bottom of Government Exhibit

1202-18.

A. So, the top's kind of like I just described, that this is, like, a pop-up box that would have popped up. It can be, like, if it says show warn on people's left, like, show warn, show warning message. If we look at the bottom here --

Q. Sorry. Just before we do that, Mr. Leedom, what does the line below "show warn" indicate?

A. The property collector line?

Q. Yes. I'm sorry. The one that starts "VI client soap tran."

A. I think the -- I think that's just the type of log that the -- like, soap is a -- how am I going to -- too detailed. Soap's just the type of protocol that the client talks to the server with. So this is just saying that this is -- this is just kind of describing that connection.

Q. And then what ultimately did happen here?

A. Look at the bottom half, the little bottom part of the blown-up command. This says that the snapshot reversion was successful.

Q. At what time?

A. 4:20, 2016, at 5:35.

Q. So let's talk about the effects of that, Mr. Leedom.

MR. DENTON: If we could go to page 102.

Q. Prior to the reversion, which SSH keys have administrative access to the Confluence virtual machine?

A. Prior to the reversion, there was only one.
Q. And is that what's depicted in Government Exhibit 1207-18?
A. Yes.
MR. DENTON: Go to page 103, Ms. Cooper.
Q. After that reversion, which SSH keys have administrative access to the Confluence virtual machine?
A. All seven of these.
Q. Are those the seven that were present on April 16, 2016?
A. Yes.
MR. DENTON: Can we go to page 104, Ms. Cooper.
Q. What is the first SSH key with administrative access to the Confluence virtual machine there?
A. This is Josh Schulte's SSH key.
MR. DENTON: Can we go to page 105, please.
Q. Mr. Leedom, can you summarize the effects of the defendant's reversion to that BKUP 4-16-2016 snapshot?
A. Yes. So, the first step, kind of like I mentioned multiple times before, is when you go back to that 4/16 snapshot, all of those old admin passwords are now valid again. This gave Mr. Schulte, like, full administrative access both through the SSH key as well as the username/password to that Confluence virtual machine. We know that the virtual machine had a mount point to the Altabackup server. You saw that earlier. And --
Q. Sorry, Mr. Leedom. Can I just stop you there?
A. Sure.

Q. Can you explain a little more about what a mount point actually is?
A. Sure. Like, when I say mount point, earlier on, we saw the -- when the -- how the server mounts that or attaches to that Altabackup file share; the mount point is just essentially the holder on the server where you'd go to access it.
Q. And what does it mean that there was a mount point with access to the Altabackups in the Confluence virtual machine?
A. So, that's one of the few places on this DevLAN network where you could actually access those backups.
Q. I stopped you before the last bullet. What's that?
A. So, actually, it's very similar to what I just said, which is that without administrative access to one of these few places on the network that could access those backups, you wouldn't be able to do it.
MR. DENTON: So, again, if we could go to page 106.
Q. And Mr. Leedom, explain to us a little bit where we are in the time line of that evening's events?
A. So, we're still pretty close to the beginning here. We've just reverted to the 4/16 backup to where all those passwords are the old passwords.
Q. Did you determine any other related activity with the Confluence virtual machine by the defendant that evening?
A. Yes.
MR. DENTON: Let's go to slide 107, Ms. Cooper.

Q. What's shown here, Mr. Leedom?
A. So, we're kind of going forward to the end of this period on the time line, when Schulte, like, re-reverts or restores the Confluence machine to that BKUP snapshot that he took before he started doing all this.
Q. If you could just walk us through what's shown in Government Exhibit 1202-19.
A. So, this looks pretty similar to what we saw before. This is a log from the, from Mr. Schulte's workstation for that vSphere application. The first thing we see is another warning message that says the current state of the virtual machine will be lost unless it's been saved in a snapshot. Revert to snapshot BKUP. So this just is confirming in a little pop-up box to say are you OK with, like, throwing away everything that's happened on this virtual machine and restoring it to whatever state it was in when this snapshot was taken. We see a log that starts the reversion and finishes shortly thereafter.
MR. DENTON: If you could go to page 108, Ms. Cooper.
Q. Mr. Leedom, were you able to find any records of what happened between 5:29 p.m. and 6:51 p.m. in the Confluence virtual machine?
A. No.
Q. Why not?
A. Because Mr. Schulte deleted that snapshot, and since he

reverted to the snapshot, it erases all activity for that virtual machine for the time frame.

Q. You talked about unallocated space before. Was there any unallocated space for the Confluence virtual machine that you could analyze?

A. No.

Q. Why not?

A. Because it would have been in the deleted portion of the snapshot, because it's all -- it's all, like, stateful, so if it's all deleted, it's not there.

Q. What do you mean by stateful?

A. The way snapshots work, I alluded to it a little earlier, they're kind of built off of each other in, like, the delta or differences. So based on, like, what types of snapshots are available in time, you can have access to different things, but with the way that the defendant reverted to an old one -- well, made a new one, reverted to an old one, did some stuff, and then deleted the new one after -- after reverting, going back to the new one, it erases all activity that was occurring at that time. It's a little confusing, but --

Q. Let's keep going, Mr. Leedom, for a second, and look at page 109. After reverting back to the BKUP snapshot, what did the defendant do next with the Confluence virtual machine?

A. So, this is an exhibit showing from his workstation in vSphere, he clicked the, the, like, the available snapshots

window, so just viewing all available snapshots.
Q. And how many snapshots were present at 6:51 p.m. on April 20, 2016?
A. Three snapshots.
MR. DENTON: Then let's go to page 110.
Q. What did the defendant do with the BKUP snapshot he had created?
A. He deletes it.
Q. Explain what's shown here in Government Exhibit 1202-21.
A. So, same log file from Mr. Schulte's workstation for vSphere. Similar to last time, there's a little warning box that pops up, says are you sure you want to delete the snapshot? Yes, no. Clicks yes, and it deletes it.
Q. Now, you talked a little bit about the effect of the reversion to that BKUP snapshot. What effect, if any, did deleting that snapshot have?
A. It completely, like, removes that point in time and, you know, it's kind of like the part of covering your tracks. Like if someone else had looked at this list of snapshots, and you couldn't figure out, like, oh, well, who made this other snapshot, it shows that someone was accessing the server.
MR. DENTON: If we could go to the next slide, 111.
Q. After this period of time, Mr. Leedom, that's depicted in the white boxes up here, did the defendant have administrative access to the Confluence virtual machine?

A. After the snapshot -- after it was re-restored and deleted?
Q. That's correct.
A. No.
Q. What about in between?
A. Yes, he did, in between.
Q. Did you identify any relevant activity during that time period when the defendant had administrative access to the Confluence virtual machine?
A. Yes.
MR. DENTON: Let's go to the next page, please, Ms. Cooper.
Q. What was that activity?
A. So, one of the first things that happens is we know from the access times, from the Confluence backups, that they were accessed at 4/20, 5:42, and they were accessible from that Confluence virtual machine. So it's my opinion that they were copied at that time by the defendant.
Q. Now, you said that was your opinion, Mr. Leedom. Do you know that at some point these files were, in fact, copied?
A. Yes.
Q. How do you know that?
A. Because we've been able to determine that it's these exact files that WikiLeaks used to publish their publication.
MR. SCHULTE: Objection.
THE COURT: Overruled.

BY MR. DENTON:

Q. Were you able to find a particular command to copy these files?

A. No.

Q. Why not?

A. Because any evidence of commands run to do this being accessed from that Confluence virtual machine, with the way that the snapshot restorations happen and that activity being erased, there's no -- there's no way to recover that information.

Q. So is that activity that would be recorded in the Confluence virtual machine itself?

A. Yes.

Q. Not on the ESXi server?

A. No, for the most part.

Q. And not --

A. For the commands, yes.

Q. And not on the client workstation?

A. Correct.

Q. What effect, if any, did the reversion have on the defendant's ability to access these backups?

A. The 4 -- oh, well, once he restored it?

Q. Yes.

A. After that, he doesn't have administrative access to anything anymore, except to the ESXi server, which we just saw.

To get access, he had to go through this rigmarole of doing the snapshot reversions, so he wouldn't have access.

MR. DENTON: If we could go to page 113, Ms. Cooper.

Q. And again, just to orient us, Mr. Leedom, how long was that after the defendant's reversion to BKUP 4-16-2016?

A. Less than ten minutes.

Q. We're going to shift gears and talk about what the defendant did with log files. Before we get into the specific commands, did you find any evidence that the defendant deleted log files from his Windows workstation itself?

A. No.

Q. Was that significant to you?

A. To some extent, yes.

Q. How so?

A. I mean it was very suspicious to see, like, so much work involved with deleting log files from the ESXi server, the snapshot reversions. But all of those vSphere logs that we were looking at, the VI client logs, those were all still intact on his workstation.

Q. Did you come to an opinion about why those remained on his workstation?

A. Yes, I did.

Q. What was that?

A. I don't think he knew where to find them.

Q. If the defendant had copied something on April 20 through

the Confluence virtual machine, would that have been recorded on his Windows workstation?

A. No.

Q. As a general matter, were you able to draw any conclusions about a pattern of log file deletions over the course of the evening of April 20?

A. Yes.

Q. What was that?

A. It's evident that Mr. Schulte was trying to cover his tracks about, you know, all the activity that had been going on for the last hour or so on that server.

Q. Let's go through some of those, if we can.

MR. DENTON: Can we go to page 115, please, Ms. Cooper.

Q. Just to remind us how these log commands work, Mr. Leedom, what are we taking a look at here?

A. So, this is just another file listing of the log file folder on the ESXi server, same as before, that show everything in a list and time sorted reverse order.

MR. DENTON: If we can go to the next slide, actually, Ms. Cooper.

Q. Again, is that the command that's being shown in the top box here?

A. Yes, it is.

Q. Is that total reflected there higher than it was earlier in

the evening?
A. It is.
Q. Did you draw any conclusions as to why that is?
A. I mean the machine's been running and the, with all the snapshot activity, machine changing, like, that increases it's amount of logs, so --
Q. Is there a time stamp for this particular command?
A. No.
Q. Were you still able to approximate when it was run?
A. Yes.
Q. Again, just briefly, how did you do that?
A. From the same method as before. We can look at some of those recently modified files, and knowing that, like, host D is another file that's updated frequently, so that we can use that modified time stamp to roughly time stamp and estimate when this command was run.
Q. And where did this log come from?
A. So, this exhibit came from the -- Mr. Schulte's virtual machine from unallocated space.
Q. And what conclusions were you able to draw from that?
A. So, we know that he was clearly using that virtual machine to access this ESXi server. Like I mentioned before, we're not just getting, like, the name of the commands that he ran. We're actually getting the output from the commands, so we're actually seeing the same thing he saw when he ran those.

Q. So just looking at the bottom here, the last entry there, that's hostd-probe.log --

A. Yes.

MR. DENTON: If you could go to page 117, Ms. Cooper.

Q. -- what did the defendant do immediately after running that list command?

A. He runs the RM or the remove command, which is the command to delete files.

Q. And what type of files did he delete?

A. These are all log files for the ESXi server. They have various, different purposes, but --

Q. Were some of those files ones that would have been significant to your forensic analysis?

A. Very significant.

MR. DENTON: Go to page 118.

Q. What would have been some of the significant files that the defendant deleted on April 20, 2016?

A. So, in order of, I guess, like severity or usefulness, VM kernel's No. 1, so -- do you want me to just describe each of these?

Q. Please, Mr. Leedom.

A. So VM kernel is the main log file for everything, like, low level that happens, like, on the server -- networking information; drivers; when virtual machines are turned on or turned off; storage changes. Everything like that is going to

be stored in there. So it's, like, the core system logs.
Q. And then what about host D?
A. So, host D we've seen a lot of these in the presentation. This has a lot of that server-side logs for the communication from vSphere, that client application. It's got, like, log-ins from those. It's got events that happened related to, like, to, like, vSphere.
Q. And then what about syslog down at the bottom here?
A. So, syslog, another really important log. We use it a lot for forensic analysis. This is like all your system management logs, so changes that are made to the server. It's kind of the, like, general catchall for most logs on a Linux system.
Q. And just to be clear, Mr. Leedom, what's depicted in black next to the descriptions of each of those logs?
A. This is just an excerpt from the previous exhibit just showing the remove command that the defendant used to delete each of these files individually.
Q. Now, you said these were files that would have been significant to you in forensic analysis, is that right?
A. Yes.
Q. Did the defendant also delete files that would not have been significant to you?
A. He did.
MR. DENTON: Go to page 119, Ms. Cooper.
Q. What were some of those files?

A. I'll run through these really quick. So, I don't want to say these weren't, like, these were totally insignificant files. I think everything we review in an investigation has some level of significance. But from a, like, just from kind of trying to understand how well the defendant knew how to use the server, knew what these logs were for, and seeing that, you know, he also chose to delete these as well as some of the other, more important files, it kind of shows that he's just going for, like, kind of a scorched-earth approach to delete everything that was touched in the last hour, opposed to only deleting, like, the few key logs that would have, like, all the juicy bits.

So to kind of go through these three as an example, storage -- storage RM is just, like, storage data logs. Rhtproxy, this is, like, proxy connection information. I think a lot of these also aren't very big, and the content in them isn't super valuable from a investigative perspective.

VPXA, these are logs related to a web service that ESXi runs.

Q. So, let's look at, again, where we are on the time line, Mr. Leedom.

MR. DENTON: Go to page 120.

Q. Approximately what time were those first log file deletions?

A. About 5:55 p.m.

Q. And following that, did the defendant run more commands?
A. Yes, he did.
MR. DENTON: Go to page 121.
Q. Is this the box showing sort of the end of those remove commands that we were looking at earlier?
A. Yes.
Q. What did the defendant do next?
A. So, he lists the log files, lists the folder of log files.
Q. And what's the total that's depicted there?
A. It's 17413.
Q. I'm not going to ask you to do math, but is that smaller or bigger than it was before the deletions?
A. It is smaller.
Q. What, if any, conclusions are you able to draw from that?
A. That these log deletions were successful.
Q. Is it accurate to say that data was no longer available on the ESXi server?
A. Yes.
Q. Again, just looking at this here, without a time stamp, are you able to tell approximately when this list command was run?
A. Yes.
Q. What time was that?
A. So, look at shell.log here for 5:57 p.m. on April 20.
MR. DENTON: And if we could go to page 122, Ms. Cooper.

Q. What did the defendant do next?
A. He deletes some more log files.
Q. Now, there's a pretty wide range here, from 5:57 to 6:16 p.m. Why is that?
A. There's only so many list commands that we can use to roughly time stamp this. So until the defendant runs another one, we can't really very accurately time stamp exactly when these commands are run because we don't have the -- we don't have the time stamps for those commands, essentially.
MR. DENTON: If we could go to the next slide, Ms. Cooper.
Q. Is the time that's represented in the boxes here the start of the applicable range?
A. Yes.
Q. Then I want to talk a little bit more about those VI client logs that you referenced.
MR. DENTON: If we could go to page 124.
Q. You said that you reached the conclusion that the defendant didn't know where to find those log files, is that right?
A. Yes.
Q. What led you to that conclusion?
A. We actually saw him searching for those log files in the wrong place. In this case, on the wrong machine entirely. The VI client logs are for the client, meaning, like, a workstation. But he's looking for them on the server itself.

Q. Explain a little bit about what we're looking at here in Government Exhibit 1203-22.
A. So, we'll just take the first command here. It's "find." This is a Linux command to search for stuff. I'll break it down real quick. This is very short. So the first argument is slash. This says the starting directory that you're going to search in. So, a single forward slash if you use, like, a Windows computer, you might be familiar with like C, like C colon, like a C drive. It's essentially, like, the root of the file system. So this says search everywhere for any file with the name, our next argument, dash name, VI client-star. The wildcard star behaves similarly that we saw before. So this says show me any files on the entire server that start with the word "VI client."
Q. And did the defendant find anything on the server with that name?
A. No.
Q. So what happens next?
A. He tries searching for it in a different location.
Q. And what is that?
A. The -- what is the location?
Q. What is in the line below? Let me ask it that way.
A. Oh. The empty line? Or the --
Q. No. The next line with text in it.
A. OK. Sure. So, this is another find command. Instead of

it looking in the slash directory, it's looking in another directory that's underneath slash. It's kind of redundant, since he already ran it on everything. So obviously it comes up empty as well.

Q. And so what does the defendant do next?

A. He begins to look through the log folder for, at additional logs.

Q. In total, how many times do we see him looking for VI client logs in different forms?

A. That we were able to recover here in this exhibit, there's -- there's four searches specifically for VI client.

Q. And just to be clear, why were none of them successful?

A. Because those client logs are not on the server. They're on his workstation.

Q. So, again, there's no particular time for these commands; you just listed a range. Is that right, Mr. Leedom?

A. That's correct.

Q. Was there ultimately another command that allowed you to determine the end point of that range?

A. Yes.

MR. DENTON: Go to page 125.

Q. What does this show?

A. If we -- in this case, we're going to ignore everything that's highlighted in black and we're just going to look at the bottom. So this, another LS-ALTR command that's run, which

would let us get a time stamp for, you know, what time after those commands are run.

MR. DENTON: Let's go to page 126, Ms. Cooper.

Q. How were you able to tell when those commands were run?

A. We can look at the, we can both look at the shell.log file last time identified as well as in this case we're going to take a look at the dot. So, I'll explain what dot means.

In Linux, the, like, single period, like, dot character, when you do a file listing like this, it represents your current directory. And when it shows a modified time for it like this, we have a time stamp, this just means this was the last time that a file was modified in this directory. So it kind of, like, you know, aggregates everything that's inside it, and says, like, OK, well, the last thing anything in this folder was modified that this time stamp, so that's what we're going to use here to do our time stamp estimate.

Q. Let's take a look at where we are on the time line, Mr. Leedom.

MR. DENTON: If we could go to the next.

Q. After that point, did the defendant delete additional log files?

A. Yes.

Q. Which file was deleted here?

A. The hostd-probe log file.

Q. And again, was this a significant log file to you?

A. No.
Q. What, if anything, does appear significant about that log file on this page?
A. The hostd-probe log file?
Q. Yes.
A. So, I know in the earlier example, he'd actually tried -- I think it was this one. He tried to delete it but spelled it wrong, so this time he spelled it correctly.
MR. DENTON: If we could just go back to page 117, Ms. Cooper.
Q. Is that shown here on Government Exhibit 1203-29?
A. Yes, it is.
Q. Where is that?
A. It's about, like, two-thirds of the way down. You see that RM host probe instead of hostd-probe. It just says couldn't find that file, so --
MR. DENTON: Then if we can just run forward again to page 127.
A. I think there's one more thing I'd like to add on this, if I can.
Q. Go ahead.
A. So, I think, too, for this hostd-probe file, if we look, I mean it's one of the few files that are left to -- from, you know, this 5:55 time frame. There's not much else left. If you look, you can see the -- there's one from, like, 2038 and

21, 2155, for those time stamps. So it's just, it's also one of the few files that are left.

Q. So let's talk about that for a moment. The file that's listed previous to that, vmksummary.log, what's the time for that?

A. So, that would be -- I think we're right at 5 p.m.

MR. DENTON: If we could go to the next page, Ms. Cooper.

Q. Was there any modification to that log file during the time period of the defendant's reversion activities on April 20?

A. I don't believe so.

Q. Now, the log files that we've been talking about in the deletions that are referenced here on page 128, where were they located?

A. All on the ESXi server.

Q. And generally speaking, what type of activity did they record?

A. Anything happening, like, on that server or to anything on that server.

Q. Did you identify any other activity with logs in other locations by the defendant that evening?

A. Yes.

MR. DENTON: Go to the next page, please, Ms. Cooper.

Q. What does this show, Mr. Leedom?

A. So, we're still -- we're still on the ESXi server. Instead

of being in the main log folder for the whole server, we're actually in the log -- well, we're in the folder for the Confluence virtual machine. So we can tell that from -- it says INF Confluence. So inside a folder for a virtual machine, there's a bunch of files.

I guess can I really briefly explain?

Q. Please.

A. There's, like, files that represent, like, virtual hard drives, for example; a file that represents, like, the memory for the computer. That stuff's all stored as individual files. There's also log files. In this case, vmware.log is a log file that stores everything that is happening to this virtual machine.

Q. Are there also snapshots that are depicted here?

A. Yes.

Q. How many?

A. We have three snapshots, I think.

Q. And are you able to approximate what time these commands were run?

A. Yes, we can.

Q. And what time was that?

A. 6:38 p.m.

Q. What's the first command that's depicted here?

A. So, this is a -- this says remove, so delete vmware.log.

MR. DENTON: Go to page 130, Ms. Cooper.

Q. Would vmware.log have been significant to you in your forensic analysis?
A. It would be very significant.
Q. Why?
A. So, it has everything that happens to that virtual machine: if you turn it on; if you turn it off; if you change its, like, IP address; if you change what's connected to it, like what data stores are connected to it; if you take snapshots of it; it handles, like, data transfer logs in an out of virtual machine. Pretty much everything that happens to that virtual machine is stored in that log file.
MR. DENTON: If we could then look at page 131, Ms. Cooper.
Q. Did that deletion of vmware.log that we were just looking at occur before or after the defendant's reversion completed?
A. So, this is -- you're talking about when he restored it again? Or --
Q. I'm sorry. Yes. Let's call it that.
A. OK. So, he deletes the log file before he's, you know, fully cleaned up.
Q. So at the time that vmware.log was deleted, which snapshot was running the Confluence virtual machine?
A. That snapshot from 4/16, from before ISB changed the passwords.
Q. Were there any other Confluence log deletions later?

A. There were.

MR. DENTON: Go to page 132.

Q. What are we looking at here, Mr. Leedom?

A. These are some more deletions for -- ones for that same file again and another one's just for another one of those vmware log files.

Q. And it looks like there are a number of files here that end with the .log file extension, is that right?

A. That's correct.

Q. What, if anything, was unique about the two that the defendant deleted here?

A. They're just the most recent.

Q. When was vmware-9.log last written to?

A. On April 20, about -- what is that, like, 6:50 -- I'm sorry. 6:38 p.m.

Q. And what about vmware.log?

A. Similarly, April 20 at 6:51.

Q. Did significant events happen at 6:51 p.m.?

A. Yes.

MR. DENTON: Go to page 133, Ms. Cooper.

Q. Why was that a significant time?

A. So, that's when he reverts to his new BKUP snapshot and, you know, essentially kind of cleans up all the activity of what he's been doing.

Q. After the defendant deleted those Confluence vmware log

files, what happened next?
A. He -- are you saying after, like, he deletes the snapshot?
Q. After that. After the deletions at 6:56 p.m. that we were just talking about.
A. OK. I think there's some more log deletions after that.
MR. DENTON: Let's take a look at page 134, please.
Q. What does this show, Mr. Leedom?
A. So, this is showing a list of the, all of the files in this Confluence folder.
Q. And is vmware-9.log in that folder?
A. No, it's not.
Q. Is vmware.log in that folder?
A. No.
Q. Why not?
A. Because they were deleted.
MR. DENTON: Let's go to page 135, Ms. Cooper.
Q. In addition to running those commands with respect to the Confluence folder, did the defendant also delete other log files from the ESXi server again?
A. Yes.
Q. What does this show?
A. So, exhibit 1203-6 has the deletion for hostd-probe.log.
Q. Is that what we were looking at earlier?
A. Yes.
And then if we go to the bottom, we have an -- I think it's

an attempted deletion of vmware.log.

Q. Why do you call it an attempted deletion?

A. So, we saw vmware.log was inside the folder for Confluence, but now we're inside the log folder for the whole server, not the Confluence virtual machine. So I don't believe this file actually exists.

MR. DENTON: Could we go to the next page, Ms. Cooper.

Q. After that attempted deletion of vmware.log from the ESXi server, what is this next command that starts with "find"?

A. So, of the -- I'll kind of preface this, like, of the things that the defendant did that were most, like, evident of him trying to clean up for this and doing activity that wasn't normal for an admin, I think this is probably the biggest one. He's looking for all files that are newer than shell.log.

We've talked about what shell.log is. It stores all the commands that are run on the server, and like I mentioned before, usually, after you're done writing a command and you hit enter, it updates that shell.log file. So, you know, it kind of is the final way to clean up after all of this activity; he's looking for anything anywhere on the whole server that was written to newer than the last time he typed the command in.

Q. And again, were you able to review the shell.log file?

A. Yes.

Q. Were any of the commands that we've talked about that the

defendant entered on April 20 reflected in that actual log file?

A. No.

Q. Where did you find them?

A. We found them in the unallocated space on his virtual machine, like, on his desktop.

Q. And again, what conclusions were you able to draw from the fact that they were not in shell.log, but they were in unallocated space?

A. It's clear that Mr. Schulte edited the shell.log file and deleted all of that activity from the 20th.

MR. DENTON: If we could just go to page 137, Ms. Cooper.

Q. Mr. Leedom, what, if any, significance is there to the last two entries for log file deletions on the right here at 6:56 and 6:58 p.m.?

A. So, they're just the last two, you know, checks to make sure, like, OK, everything's done, let's go make sure there's nothing else to clean up, and those are the last two deletions.

Q. And so at this point in time, at 6:58 p.m., can you describe what the cumulative effect was of the defendant's reversion and deletion of these BKUP snapshot and the deletion of these various log files?

A. It erases, like, pretty much all of his activity that happened on that server for the last hour and 20 minutes.

Q. Are you familiar with vaults, Mr. Leedom?
A. Yes.
Q. To your understanding, what is a vault?
A. So, a vault -- at the agency, it's, we also might call it a SCIF. It's a, it's a room. It's, like, an office room that is designed to store classified information.
Q. And are there any special instructions that you're aware of for what the last person in a vault is supposed to do?
A. Yes.
Q. What is that?
A. So, either -- if you're the, like, the first person opening up for the day or last person leaving, you have to -- you've got to lock and close the vault.
Q. So the last of these log file deletions that you talked about was at 6:58 p.m., is that right?
A. Yes.
MR. DENTON: If we could go to page 138, Ms. Cooper.
Q. What happened at 7:07 p.m., Mr. Leedom?
A. Mr. Schulte locked up and closed the vault.
Q. What, if any, conclusions were you able to draw from that?
A. He was the last person in the office that day.
MR. DENTON: If we could go to, then, page 139.
Q. Mr. Leedom, were you able to get a complete picture of all of the defendant's activities during this time period?
A. No.

Q. Why not?
A. A lot of the activity that happened would have been inside that Confluence virtual machine or in log files that the defendant deleted.
Q. Were you still able to reach conclusions about his activity during that time?
A. Yes, I was.
MR. SCHULTE: Objection. Asked and answered.
THE COURT: Overruled.
MR. DENTON: Go to page 140.
Q. What, if any, significance did Government Exhibits 1207-27 and 1207-30 have in your conclusions?
MR. SCHULTE: Objection.
THE COURT: Overruled.
A. So, like, upon seeing the, like, date-accessed times for these backups, it confirms, you know, my opinion that the only thing happening on the network at that time was the defendant in the Confluence VM, which had access to these backups, and then all of the activity for the log file deletion, kind of the secrecy around, you know, covering all those tracks, then having the date-accessed time, which is the time stamp that's updated when you copy a file, for these, as well as seeing on WikiLeaks and doing my review of all the content there versus the content that's available on these March 3 backups, the defendant copied them.

MR. DENTON: If I could just have a moment, your Honor?

Nothing further, your Honor.

THE COURT: All right.

Cross-examination.

Ladies and gentlemen, while we're getting set up in the transition, if you want to just stretch where you are, you're welcome to stand and stretch.

(Continued on next page)

INDEX OF EXAMINATION

GOVERNMENT EXHIBITS