M6oWsch1

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

3   UNITED STATES OF AMERICA,

4   v.   17 Cr. 548 (JMF)

5   JOSHUA ADAM SCHULTE,

6   Defendant.
                                         Trial
7   ------------------------------x

8   New York, N.Y.
                                         June 24, 2022
9   9:00 a.m.

10 Before:

11
                      HON. JESSE M. FURMAN,
12
                                         District Judge
13   -and a Jury-

14   APPEARANCES

15 DAMIAN WILLIAMS
        United States Attorney for the
16   Southern District of New York
    BY: DAVID W. DENTON JR.
17   MICHAEL D. LOCKARD
         Assistant United States Attorneys
18

19 JOSHUA A. SCHULTE, Defendant *Pro Se*

20
    SABRINA P. SHROFF
21 DEBORAH A. COLSON
        Standby Attorneys for Defendant
22
    Also Present: Charlotte Cooper, Paralegal Specialist
23

24

25

                    SOUTHERN DISTRICT REPORTERS, P.C.
                            (212) 805-0300

M6oWsch1

1   (Trial resumed; jury not present)

2   THE COURT: You may be seated.

3   All right. Welcome back. Good to see everyone.

4   We're resuming trial. Before we resume Mr. Leedom's

5   testimony, anything to discuss this morning as opposed to at

6   the break or at the end of the day?

7   MR. DENTON: Yes, your Honor.

8   At least from the government, we had a couple of

9   issues related to proposed defense exhibits that we expect the

10   defendant may try to introduce with Mr. Leedom that we wanted

11   to raise. There are essentially three categories of proposed

12   defense exhibits to which we have objection, at least one of

13   which raises a separate concern.

14   First, we were provided yesterday by standby counsel

15   with six articles from the internet relating to purported

16   security vulnerabilities in various Atlassian products that

17   were identified in 2021 and 2022. But aside from the timing of

18   their production, we think there's an obvious hearsay problem,

19   to say nothing of the 401 and 403 problems of arguments

20   relating to vulnerabilities identified in different versions of

21   software long after the events that are at issue in this trial.

22   Those articles were not provided to us marked, so we don't have

23   reference numbers for them.

24   There's a related set of materials that were provided

25   to us, part last week and part on Tuesday, which were marked as

1   defense exhibits 1202, 1204, 1206, and 1207, which are

2   reference materials, also apparently from the internet, which

3   again, we think that to the extent the defendant wants to

4   cross-examine Mr. Leedom about his conclusions, he certainly is

5   entitled to do that, but he's not entitled to offer reference

6   materials into evidence.

7   The third, however, and most sort of problematic

8   category are the items that were marked as defense exhibits

9   1210 and 1211, which is code and then a compiled executable

10   program of that code that appear to have been written by the

11   defendant. That raises an evidentiary concern in the sense

12   that those are essentially his own statements, which he's not

13   entitled to offer but, separately, to us, raises a substantial

14   security concern of how the defendant was able to, first, write

15   but, more significantly, compile code into an executable

16   program on his laptop.

17   You know, your Honor, we have accepted a continuing

18   expansion of the defendant's use of a laptop that was

19   originally provided for the purpose of reviewing discovery, but

20   to us, this is really a bridge too far in terms of security

21   concerns, particularly in light of the issues uncovered during

22   the last issue with his laptop and the concerns that the MDC

23   has raised to us about tampering with the law library computer.

24   We have not taken any action in response to that, because we're

25   in the middle of trial and we're loath to do things that would

1   disrupt the trial at this point. The fact that defendant is

2   compiling executable code on his laptop raises a substantial

3   concern for us separate from the evidentiary objections we have

4   to its introduction.

5   THE COURT: OK. Maybe this is better addressed to

6   Mr. Schulte, but I don't even understand what the third

7   category would be offered for, how it would be offered, what it

8   would be offered for.

9   MR. DENTON: As best we can tell, it is a program to

10   change the time stamps on a file, which I suppose would be

11   introduced to show that such a thing is possible. I don't

12   know. We were only provided with it on Tuesday. Again, we

13   think there are obvious issues with its admissibility separate

14   and apart from its relevance, but like I said, for us, it also

15   raises the security concern that we wanted to bring to the

16   Court's attention.

17   THE COURT: OK. And with respect to the second

18   category, the reference materials, I don't know what we're

19   talking about there. Would it not fall within the scope of

20   Rule 803(18)?

21   MR. DENTON: Your Honor, I think it is possible that

22   they might. I think, on the other hand, to the extent that the

23   defendant wishes to offer materials separate and apart from

24   sort of cross-examination and through just kind of a generic,

25   you know, introduction of them, there's some foundation that's

1   still required under the rule.

2   THE COURT: Right. Well, the rule, to be clear,

3   doesn't actually allow the material to be admitted; it allows

4   the statement to be read into evidence but not received as an

5   exhibit. I don't know if that's the purpose of it. Obviously,

6   it's still required to be marked, but it wouldn't come into

7   evidence.

8   All right. Mr. Schulte.

9   MR. SCHULTE: Yeah. So, just starting with the first

10   thing about the vulnerabilities, most of this stuff is very

11   recent. We only -- it's from, some of this is from June, even.

12   So we just discovered this. As soon as we obtained it, we

13   provided it to the government. So the vulnerabilities, even

14   though the versions of the software are newer now, the

15   vulnerabilities date all the way back to very old versions of

16   the software. So we think that it's relevant to the

17   cross-examination to show the vulnerabilities in the software.

18   THE COURT: But is it your intention to offer the

19   articles, because the articles are pretty much straight

20   hearsay; no?

21   MR. SCHULTE: I mean they're not really articles in

22   the traditional sense. They're security, security documents,

23   some of which were produced through his company, we believe,

24   MITRE. Or the MITRE company's involved with this -- so what it

25   is is there's a tracking mechanism for vulnerabilities CVE, and

1   his company, MITRE, at some point was involved in this. So

2   he -- the question is -- I don't know whether or not the

3   document itself should come in. I think it's a technical

4   document. It's not really a news article. It's about tracking

5   of the vulnerabilities. So we think it should come in, but at

6   the very least, we could show it.

7   THE COURT: That's not a distinction that is

8   recognized in the hearsay rule. There's no exception for

9   technical documents. It's an out-of-court statement. I don't

10   see any reason why you can't ask the expert, are you aware that

11   this tool has a security vulnerability and has always had it,

12   if you can link it to the relevant time in this case, as

13   opposed to some version of the software that postdates the

14   events in this case by some number of years, which would be

15   totally irrelevant. I think if you can link it and you can ask

16   him directly, that's one thing.

17   What you can't do is either offer an exhibit that's an

18   out-of-court statement by someone else or ask him, isn't it

19   true that MITRE said X, Y and Z. Because that's also an

20   out-of-court statement. In other words, you can ask him

21   directly, but you can't ask about an out-of-court statement.

22   MR. SCHULTE: OK.

23   THE COURT: And I don't see a scenario in which these

24   articles themselves come into evidence. Again, maybe if you

25   say isn't it a fact that this Atlassian product had a security

M6oWsch1

1   vulnerability dating to whenever and he says I don't remember

2   that, then you can try and refresh his recollection with it.

3   But again, I don't see any scenario in which you can offer that

4   article, let alone through this witness --

5   MR. SCHULTE: OK.

6   THE COURT: -- as opposed to the reference materials.

7   Again, I would draw your attention to 803(18), which might

8   permit you, if they would qualify under that rule, to have the

9   witness read certain statements from it. But I don't see any

10   scenario in which those out-of-court statements come in either.

11   MR. SCHULTE: OK. Understood. Yeah, I think just

12   asking him about it, if he knows about it, in general, without

13   bringing in the document, I think that's --

14   THE COURT: But asking if he knows about an

15   out-of-court statement is asking about hearsay. So you can ask

16   if he knows about the fact.

17   MR. SCHULTE: OK, yeah.

18   THE COURT: Not about the statement. Do you

19   understand the distinction?

20   MR. SCHULTE: Yes, I do.

21   THE COURT: OK. And if he says no, I think you're

22   basically stuck with that answer.

23   And then the third category, Mr. Schulte, the code

24   situation, there are two separate issues there. One is the

25   security issues, which I think are separate and apart from any

M6oWsch1

1   admissibility issues, and we can take up separately if or when

2   there's an application on that front.

3   MR. SCHULTE: Yeah, and we can circle back to the

4   manuals. But for the code, the government produced lots of

5   source code in discovery, and this specific file is, like, ten,

6   ten lines of source code as well as --

7   THE COURT: Where does it come from? Did you write

8   it?

9   MR. SCHULTE: Yes, I wrote it. That's correct.

10   THE COURT: How do you intend to offer that? It is a

11   statement of your own.

12   MR. SCHULTE: Well, so, like I -- so, it may -- it may

13   help to go back to the manuals. So, there are several

14   technical manuals that he should be aware of in some technical

15   library. So based on that, what I intended to do was show him

16   those documents from Microsoft and other providers that -- he

17   should know this information, and from that I would then show

18   him the seven lines of code, ask him if he recognized -- it's

19   basically the same thing from the library, just tweaked to

20   specifically show an April 20 modification and basically ask

21   him if he knows, understands and knows what this is. It's no

22   different as if he wrote it or some other, random person wrote

23   it.

24   The point is the functionality and what the code can

25   do and how quickly it is to write something like that. I think

1   that's the point of the testimony, to get out how easy this is

2   to do. It doesn't take -- anyone can do this easily. It's on

3   the internet for how to do this. It's proper, like, expert

4   cross on that information. And then, this, I don't know from

5   there, then to have him, once he explains exactly what it does

6   or how it works, to potentially just -- it's just a

7   double-click this thing, the program, and then it just shows

8   how the file time is changed. So that, I think, is separate.

9   It's almost a demonstrative of how the source code works. But

10   I think the source code is proper for the expert to be able to

11   explain how it works, how easy it is to do. And I think the

12   demonstrative of the executable is a separate thing. But I

13   think would go -- it's just a guide to show how that works and

14   how it would show up in Windows and how the file times get

15   changed.

16   THE COURT: All right. I think what we're going to

17   have to do is take it up as it comes, see what Mr. Schulte

18   tries to do with it, mindful of the limitations on what he can

19   and cannot offer. I'm not sure the code, depending on how he

20   uses it, it may not be offered for the truth *per se*, in which

21   case I'm not sure there's a hearsay problem. But we'll take it

22   as it comes, I guess.

23   MR. DENTON: Your Honor, I think there's two issues.

24   The first is it seems like his purpose is to offer it

25   for the truth that these statements that the defendant wrote do

1   this thing that the defendant asserts they do. So I think that

2   does -- I mean we're in a little bit of a strange posture here.

3   The second issue that we have is, again, this is

4   something that was only provided to us on Tuesday morning. We

5   didn't have a chance to review it until Mr. Leedom was already

6   on cross. We only had a limited ability to see what it is and

7   figure out what it is, and that's been bound up in these

8   security issues. There's no reason this is something that

9   should be coming at this point, and so we think there's a

10   separate issue there as well.

11   THE COURT: All right. But Mr. Denton, Mr. Schulte

12   could theoretically put a white board up and say, Mr. Leedom,

13   isn't it the fact that I could write a line of code that says

14   this and I could write a line of code that says this, and it

15   would result in the log files being deleted in this way, or

16   whatever, assuming that there's a relevant conclusion there.

17   Right? I'm not sure it's different than that except that it

18   was provided in advance. Again, I don't know if it's going to

19   come in. I think we have to wait and see what he tries to do

20   with it, and I'll take up any objections at that time. I

21   appreciate the heads-up, but I think we'll have to wait.

22   MR. DENTON: That's fine, your Honor, but I think even

23   doing that would raise serious issues about the defendant

24   essentially testifying in that way by putting these things, you

25   know, statements that -- code occupies sort of a weird

1   category. Obviously, it's a little bit different, but I think

2   there's still an issue there.

3   THE COURT: And do you have any law for the

4   proposition that code is, if offered to show that code can

5   produce a particular result -- in other words, that it results

6   in a computer doing something -- that that's a statement

7   offered for its truth? Because it seems to me that's more in

8   the nature of a command, and that obviously wouldn't be

9   hearsay.

10   MR. DENTON: So, I think admittedly, your Honor, there

11   is not law on this particular issue. I'm not aware of anything

12   that sort of presents this kind of analogy.

13   Again, we recognize that what the Court wants to do is

14   take it as it comes, so we'll be prepared to do that.

15   THE COURT: All right. And what are the reference

16   materials? What were those exhibit numbers again?

17   MR. DENTON: 1202, 1204, 1206, and 1207, which, I

18   think it's a little bit difficult to put them in the 803(18)

19   category because they are essentially sort of user guides

20   published or, you know, promotional materials published by

21   various companies for these products. Again, we're happy to

22   take it as it comes based on Mr. Schulte's cross-examination.

23   It's obviously fine for that to inform his cross-examination

24   and to ask questions premised on it. Our principal objection

25   is to the introduction of the materials.

M6oWsch1

1   THE COURT: Again, I don't see how they would be

2   admitted as exhibits themselves, but depending on the

3   foundation that's laid, he may be able to elicit things that

4   are in it from Mr. Leedom under the rule.

5   All right. Anything else that we have to take up now?

6   There are a couple of matters the government raised in

7   two classified submissions yesterday that I think we should

8   discuss in closed session this afternoon as opposed to here,

9   although, Mr. Schulte, to the extent that one of them pertains

10   to issues that may come up on cross, I would urge you to be

11   careful and mindful of what the government has said in that

12   letter. But anything that we need to discuss this morning?

13   MR. DENTON: Not now, your Honor. Thank you.

14   THE COURT: Mr. Schulte, can we get the witness and

15   the jury?

16   MR. SCHULTE: I mean I think there's a, an issue here

17   because some of my cross pertains to one of those issues that

18   the government is kind of raising for the first time. They've

19   been public. There have been public filings on this. I mean I

20   don't know if the government's saying that the acronym's

21   classified.

22   It puts me in a difficult position because I have,

23   maybe, several cross questions based on this that I don't think

24   is classified, has never been alerted to be classified. It's

25   in public filings. So I was just talking to them before. I'm

M6oWsch1

1   not sure what they're trying to say is classified. So I don't

2   know if there's some way to quickly just clear this up.

3   THE COURT: Mr. Denton, mindful that we're in open

4   session, I don't know what we can --

5   MR. DENTON: The acronym, AFD, has been declassified.

6   The substance of work related to that or other details of it

7   remains classified and has only been produced in classified

8   discovery. We've been careful about what has been said in the

9   public filings. We don't think it's crossed that line, mostly

10   because it's been demands by the defendant for documents which

11   the government understands do not exist, so there hasn't been a

12   need to engage on that substance in any public filings. But

13   the substance of the material has always been marked and

14   provided as classified.

15   THE COURT: OK. That's certainly consistent with my

16   impression.

17   Mr. Schulte.

18   MR. SCHULTE: I think my questions would just be kind

19   of consistent with some of the questions I've asked before,

20   basically relating to the expert's work with AFD and, you know,

21   if he's aware of some of the reports and findings that the AFD

22   has, has had.

23   THE COURT: OK. Well I think --

24   MR. SCHULTE: That's OK, right? Or --

25   THE COURT: Well, to the extent you're citing a third

1   party's out-of-court statement, there's a hearsay issue --

2   MR. SCHULTE: Right.

3   THE COURT: -- separate and apart from the classified

4   issue, so that doesn't seem OK to me. And I'm not sure what

5   relevance crossing this witness about his knowledge of an

6   office that may or may not, what that office does when it

7   doesn't pertain to his investigation would have.

8   MR. SCHULTE: Right. So, no. He specifically worked

9   with them, so just the question would be were you able to,

10   through your work with this, with AFD, did you, were these the

11   conclusions you reached? So it's specifically through his

12   forensic examination and his forensic work with AFD, they

13   reached certain conclusions, technical conclusions together.

14   THE COURT: OK. Well, I think there's another

15   question asking this witness about the technical conclusions

16   that he reached, but I don't see why that requires delving into

17   what AFD does or is or what conclusions it may or may not have

18   reached, again, much of which would be hearsay in any event. I

19   urge you to be careful. It doesn't sound like anything you

20   want to ask him would necessitate getting into the particulars

21   of what AFD does, let alone any conclusions he's drawn, and you

22   can certainly ask him directly about conclusions that he has

23   drawn. But I think we'll leave it there for now.

24   MR. SCHULTE: OK, yeah.

25   THE COURT: All right. Let's get Mr. Leedom and the

M6oWsch1

1   jury, please.

2   (Continued on next page)

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

M6oWsch1   Leedom - Cross

1   (In open court)

2   PATRICK THOMAS LEEDOM, resumed.

3   (Jury present)

4   THE COURT: You may be seated.

5   Good morning, ladies and gentlemen. Welcome back.

6   Thank you for being here on time this morning. Sorry we're

7   getting off to a slightly later start than I would like, but I

8   appreciate your being here. I hope you had a nice midweek

9   break and got back to your regular lives for a couple days.

10   We'll pick up where we left off, with

11   cross-examination of Mr. Leedom.

12   Mr. Leedom, I remind you that you remain under oath.

13   I'll also ask you at this time to remove your mask and also

14   just remind you to speak loudly, slowly, clearly, and into the

15   microphone.

16   THE WITNESS: Yes, sir.

17   THE COURT: With that, Mr. Schulte, you may proceed.

18   CROSS-EXAMINATION CONTINUED

19   BY MR. SCHULTE:

20   Q. Good morning.

21   A. Good morning.

22   Q. I'll start with admitted Government Exhibit 1207-36.

23   Exhibit 1207-36 shows the contents of the Altabackup directory,

24   correct?

25   A. Correct.

M6oWsch1   Leedom - Cross

1   Q. This is where the backups are stored, correct?

2   A. That's correct.

3   Q. Now, you testified on direct about a snapshot and a

4   reversion, correct?

5   A. Correct.

6   Q. For the purposes of the next few questions, I'm going to

7   refer to this as the snapshot reversion theory. OK?

8   A. OK.

9   Q. And it's fair to say that the thrust of your testimony on

10 this issue rested on the premise that there were strict access

11 controls to this directory and its data, correct?

12 A. A piece of it, yes.

13 Q. I mean that's the whole purpose of it, isn't it?

14 A. Of accessing, of whether or not you accessed it using the

15 virtual machine, because that's the only place it could be

16 mounted?

17 Q. That was your testimony, right?

18 A. Correct.

19 Q. And it's your working hypothesis that the Altabackup

20 directory could not be accessed because of strict access

21 controls, correct?

22 A. That's correct.

23 Q. And because one could not access Altabackup, one needed to

24 resort to taking a snapshot and undertaking a reversion,

25 correct?

M6oWsch1   Leedom - Cross

1   A.   That's one method, yes.

2   Q.   And it's fair to say that if one could access the directory

3   shown in 1207-36, then a snapshot reversion is irrelevant,

4   correct?

5   A.   Yes.

6   Q.   OK. So the safest way to determine access controls is

7   through forensic analysis, correct?

8   A.   It's one method, yes.

9   Q.   Well, that's the easiest or safest way to do it?

10   A.   I mean you could review the, like, the permissions on the

11   folder. I guess you could call that forensic analysis, yes.

12   Q.   Viewing a folder, yeah, but the CIA gave you full access to

13   everything on DevLAN. Correct?

14   A.   Correct.

15   Q.   And in fact, you listed access controls for other

16   directories on that Altabackup server, correct?

17   A.   That's correct.

18   MR. SCHULTE: I'm going to show what's admitted as

19   1207-49.

20   Q.   So this shows several of the directories on the Altabackup

21   server, correct?

22   A.   Correct.

23   Let me take that back. It's on the file share. It's not

24   the Altabackup share. The shares are very distinct and

25   different.

M6oWsch1   Leedom - Cross

1   Q.   It's on the same server?

2   A.   The same file server, yes, that NetApp file server.

3   Q.   OK.   And now, 1207-50 is the properties tab of one of those

4   folders, the source code and binary Gold copies, correct?

5   A.   Correct.

6   Q.   OK.   And admitted 1207-52, this shows access controls,

7   right?

8   A.   It does.

9   Q.   We've talked a lot about access controls, and this is just

10   a great way to show what that means, what we've been talking

11   about, right?

12   A.   Yes.

13   Q.   And these are access controls specifically for this

14   directory source code and binary Gold copies, right?

15   A.   Yes, that's correct.

16   Q.   We have different -- we can see the types in this column,

17   right?   This is an allow list, right?

18   A.   Yes.

19   Q.   The group or the individual users listed under the

20   principal column, right?

21   A.   Yes, that's correct.

22   Q.   And then the access is here.   So we have several different

23   types: Read access, so someone can actually look at the

24   documents, right?

25   A.   Yes.

1   Q.   Read and execute, and full control, and that encompasses

2   everything. You can write to the folder, you can edit the

3   documents, everything, right?

4   A.   Correct.

5   Q.   OK.   Inheritance and then what it applies to, other

6   subdirectories and the files and basically how the allow-access

7   control applies, correct?

8   A.   Yes, that's correct.

9   Q.   So if you run the same tests on the Altabackup directory,

10   what permissions are listed?

11   A.   Well, you can't really run the test the same way.

12   Q.   And why is that? You can't pull this up on the Altabackup

13   directory like this?

14   A.   Well, you could in the environment that this was being,

15   like, reviewed in, but it was shared differently. The share

16   for Altabackups was an NFS share, which is very different than

17   the type of protocol used to share the folder that we're

18   looking at right now, and, like, the home folder and other

19   folders. It's very different. The way permissioning works,

20   it's very different.

21   Q.   OK. But you can still pull up access controls such as this

22   for shares like that, right?

23   A.   That share wouldn't be able to be, like, mounted in this

24   way. You can -- you can, like, pull up access to it and I

25   think it would probably just say, like, you just have to be

M6oWsch1   Leedom - Cross

1   root to access it, but you would have to be on the allow list

2   for the actual server to be able to mount it in the first

3   place. It's just -- it's very different. It's not a, like, a

4   Windows share, so the permissions and things like that are

5   different.

6   Q. So I'm asking, though, the access controls for that

7   directory, no, I understand it's not the same as this, but just

8   similar, you can have similar types of access controls. And

9   what were those access controls on the Altabackup directory?

10   A. So, from what I understand, from the, like, when we got

11   there and the available configuration of that file server, you

12   know, a year later, when we got there, the Altabackup share was

13   just, like, I think you just had to be, like, root to access

14   it. But from everything else we've reviewed, not only do you

15   have to be root, but you have to be root and you have to be on

16   the allow list. Like, your computer would have to be in that

17   allow list for IPs, which is pretty standard for how NFS

18   servers are usually set up.

19   Q. I'm just asking specifically during this type, April 2016,

20   what were the access controls? Do you have a document that

21   shows what the access controls were for that directory?

22   A. Altabackup in 2016?

23   Q. Yes.

24   A. No, no. You have to talk to, I guess, ISB. They were

25   managing it at the time. But there's no, like, historical

M6oWsch1   Leedom - Cross

1   audit for the NetApp for -- for that.

2   Q. So you have no -- you have no ability to testify about what

3   access controls existed on this directory in 2016, is that

4   correct?

5   A. No, because we can use things -- like, when you attempted

6   to mount it on the ESXi server and we saw that that failed,

7   that shows that there was access control enabled on that share.

8   Q. We'll go into the data store in a little bit, but

9   essentially, you're not relying on any document or any

10   technical access control list; you're just inferring from what

11   you've reviewed, is that correct?

12   A. Right. You got to look at everything as a whole.

13   MR. SCHULTE: OK. Let's take a look at the data

14   store. I think this is slide 58 in your presentation.

15   Q. This is what you're referring to, right?

16   A. That's correct.

17   Q. And the data store is essentially just the way it sounds, a

18   storage space for data, right?

19   A. It's -- yeah, it's like an object that you can use to

20   access data, whether it's on the server itself or in a remote

21   location; in this case, a remote location.

22   Q. And it basically just gives you a new folder to store data?

23   A. Essentially, yes.

24   Q. OK. Creating a data store is a typical administrative

25   function, right?

M6oWsch1   Leedom - Cross

1   A. Yeah, it's something you would do to manage the -- manage

2   the server.

3   Q. And in fact, the Altabackup data store previously existed

4   on the ESXi server, correct?

5   A. I don't believe so.

6   Q. Did you review the forensic logs about the data stores on

7   ESXi?

8   A. I did.

9   Q. And did you see that there was a data store for Altabackups

10   previously mounted?

11   A. The only data store Altabackups that I remember seeing is

12   this exhibit here, 1209-7.

13   Q. This is the only thing you've seen about the Altabackups?

14   A. This is the only thing I've seen about an Altabackup data

15   store --

16   Q. OK.

17   A. -- on ESXi.

18   Q. Regardless, the failure here to create the Altabackup data

19   store does not necessarily tell you anything about the access

20   controls on Altabackup, correct?

21   A. Oh, I disagree.

22   Q. You disagree with that?

23   A. Yes.

24   MR. SCHULTE: All right. Well, let's go back to slide

25   57, right before here.

M6oWsch1   Leedom - Cross

1   Q. So here, you testified on direct that I log in as a regular

2   user, correct?

3   A. That's correct.

4   Q. OK. Using my own credentials, correct?

5   A. Yes.

6   Q. And you testified on direct that this regular user account

7   is not an administrative account, correct?

8   A. From what I understand, yes.

9   Q. So the failure to create the data store could and most

10   likely occurred because a regular user simply does not have

11   access to perform the mount, correct?

12   A. Well, the type of error that we received -- if you go back

13   to the other --

14   Q. Well, no. I'm just asking based on this. If you're a

15   regular user, you're not going to have the ability to be

16   creating and mounting directories, right?

17   A. I'm not sure exactly, because there -- I don't think I had,

18   like, audit for the user individually, like, at that level on

19   that server. So I don't know if there's, like, a, you know, an

20   explicit permission for data store management or not. But from

21   the type of error that is shown, it leads me to believe that's

22   more of a -- the NFS server actually denied the request and not

23   the ESXi server saying you don't have the correct permission

24   to, you know, create a data store. It was a -- the NFS server

25   itself said I'm not going to let you do this, if that makes

M6oWsch1   Leedom - Cross

1   sense.

2   Q.   Well, I mean error messages can be misleading, correct?

3   A.   Sometimes. I think in this case it's pretty clear.

4   Q.   I mean you just -- your testimony is -- you're just

5   speculating based upon a single error message here and a single

6   failure, correct?

7   A.   I mean it says it was denied by the NFS server. It doesn't

8   say it was -- like, it doesn't say something like you don't

9   have permission to create a data store. That's how I'm drawing

10   my conclusion.

11   Q.   But it also doesn't say that -- it doesn't say anything

12   about what or how much access controls the NFS server even has,

13   right?

14   A.   No. That wouldn't be in an error message.

15   Q.   You're also aware that OSB had its own subnet, correct?

16   A.   Just from, like, a networking perspective. I don't know --

17   I'd have to refer to, like, the network documentation.

18   Q.   Well, here, we can look at slide 52, and we're showing --

19   this is the IP address, 10.3.2.35, correct?

20   A.   Correct.

21   Q.   And this is on the 10.3.2.1 network, correct?

22   A.   That's correct.

23   Q.   OK. And we know the Altabackup is on a different network;

24   it's on the 10.3.1 network, correct?

25   A.   I believe -- I think I just remembered it ended in like,

M6oWsch1   Leedom - Cross

1   dot-70, I think.

2   Q.   You don't remember it being --

3   A.   Yeah, 10.3.1.70.

4   Q.   Yeah. That's a different network, right?

5   A.   It's a different subnet. I mean they're obviously

6   connected. To the extent of, like, which IP ranges or in which

7   subnet and how they're connected, I can't really speak to.

8   Q.   The failure here could simply be that this is on

9   essentially a different network, correct?

10   A.   I mean we know that the other servers had access to it. I

11   mean without network logs, can't really speak to that.

12   Obviously, the ESXi server was able to speak to the NFS server,

13   because the log says the NFS server denied it. So that

14   connection is definitely being made here. So I wouldn't say

15   it's being blocked by some kind of firewall or something on a

16   different subnet, but --

17   Q.   OK. But the configuration for the NFS could simply be not

18   to share with this subnet or to only share within its own

19   subnet, right?

20   A.   Could be. That's kind of how, one way you could set up the

21   allow list. You can say block a whole subnet. You can say

22   only allow certain IPs.

23   Q.   And if it was set up that way, every other user, or most

24   everyone else who's on the same regular network would then have

25   access to the Altabackup directories, correct?

1   A.   No, that's not how -- that's not how it works.

2   Q.   That's not how what works?

3   A.   If you have a explicit allow list -- I mean you can have

4   both. You can have a deny this entire subnet and only allow,

5   like, certain machines from another subnet. There's no reason

6   you can't have both.

7   Q.   Yes, but it could be configured just to deny from the OSB

8   subnet; it could be configured to allow from the regular

9   network, 10.3.1, correct?

10   A.   I guess the only, like, real conclusion I want to draw from

11   those permissions is it seems to me from my review that the

12   most likely setup for that share was that it was allow-listed

13   explicitly for the servers that needed to back up to it.

14   Q.   What is that based on, though?

15   A.   Well --

16   Q.   What forensic evidence or what evidence do you have to base

17   that conclusion on?

18   A.   Well, both speaking to the admins themselves from ISB as

19   well as their log like this. I mean it's -- put that together,

20   it's very telling.

21   Q.   Speaking with the admins, you're talking Dave, Dave C.,

22   right; he was one of those?

23   A.   Yeah, Dave.

24   Q.   And he was an employee who put the Stash on a hard drive,

25   correct?

M6oWsch1   Leedom - Cross

1   A.   I know I've heard some of that. I don't know exactly the

2   situation around that, but --

3   Q.   But that, basically this hard drive with Stash was lost,

4   correct?

5   MR. DENTON: Objection.

6   THE COURT: Sustained.

7   BY MR. SCHULTE:

8   Q.   Well, to this day, no one knows where that hard drive is,

9   right?

10   MR. DENTON: Objection.

11   THE COURT: Sustained.

12   BY MR. DENTON:

13   Q.   OK. Dave C. is the one who set up the Altabackup share,

14   correct?

15   A.   I don't know if he's the one who, like, first set it up. I

16   know that he worked on, like, the infrastructure and managed

17   it. I don't know actually who set it up initially.

18   Q.   Well, Dave C. set up the Altabackups without any access

19   controls, right?

20   MR. DENTON: Objection.

21   THE COURT: Sustained.

22   BY MR. SCHULTE:

23   Q.   You would agree that the access controls to Altabackup are

24   critical, right?

25   A.   Yes.

M6oWsch1   Leedom - Cross

1   Q. As part of your investigation, you spoke to Dave C., right?

2   A. I don't think I spoke to him, like, directly, like, face to

3   face.

4   Q. So for the access control, greater access control means

5   fewer people would have access to the data, correct?

6   A. I'm sorry. Could you say that again?

7   Q. Greater access control or more refined or more access

8   controls typically means fewer people have access to the data,

9   right?

10   A. That's correct, in general.

11   Q. And the opposite is true also -- if there's none or very

12   limited access controls the access is less controlled, right?

13   A. On principle, yes. I think there's something else to

14   unpack there, but yes.

15   Q. So what -- based on your forensic analysis, what evidence

16   did you find or what forensic evidence did you find to suggest

17   that there were more refined or more restricted access controls

18   rather than very basic, limited access controls, like limiting

19   OSB subnet?

20   A. Just for Altabackup?

21   Q. Yes.

22   A. I mean we're looking at the main piece of evidence that I

23   have that, you know, that we have that kind of supports that,

24   is the -- we can see that the data store failed to mount, and

25   there was a message from the NFS server that said there was a

M6oWsch1   Leedom - Cross

1   failure.

2   Q.   Right. But the point is that message would occur if only

3   the OSB subnet was denied. If the only access controls in

4   Altabackup was deny OSB or deny to any subnet besides the

5   network it's on, you would see this message, right?

6   MR. DENTON: Objection.

7   THE COURT: Sustained.

8   Let's move on, Mr. Schulte.

9   BY MR. SCHULTE:

10   Q.   OK. Just to be clear, for the access controls here, you

11   have no documentation or no configuration files showing the

12   exact access controls, right?

13   A.   We do not have a configuration file for Altabackup from the

14   NetApp that, like, shows the -- the allow or block list. It

15   just wasn't available at the time.

16   Q.   All right. And on that same point, as part of your

17   investigation, you were not able to conclude absolutely,

18   forensically, that there were strict access controls on the

19   Altabackup directory, correct?

20   A.   I disagree. Just --

21   Q.   I mean you're just basing it off this one finding, but you

22   don't --

23   A.   This finding and knowledge of the network and what I've

24   heard from the admins on the network.

25   Q.   What you've heard from the admins, though, I mean --

M6oWsch1   Leedom - Cross

1   (Defendant conferred with standby counsel)

2   BY MR. SCHULTE:

3   Q. What you heard from the admins is not forensic, correct?

4   I'm just talking about forensics.

5   A. It's not, like, an artifact on the network, but --

6   Q. There's no artifact on the network that says that these

7   were access controls, and you are just speculating as to what

8   the access controls are, correct?

9   MR. DENTON: Objection to form.

10   THE COURT: Sustained as to form.

11   (Defendant conferred with standby counsel)

12   BY MR. SCHULTE:

13   Q. There are no forensic artifacts, correct, that specifically

14   restrict the access controls to the directory? Right? Again,

15   you're just -- let me just be clear. You're just -- based on

16   this one piece of evidence, you're speculating and that you

17   could be wrong, correct?

18   MR. DENTON: Objection to form.

19   THE COURT: Sustained as to form.

20   (Defendant conferred with standby counsel)

21   BY MR. SCHULTE:

22   Q. OK. The only forensic artifacts -- there's no forensic

23   artifacts about the specific access controls; however --

24   THE COURT: Let's start that one over. Sustained as

25   to form again.

M6oWsch1   Leedom - Cross

1   (Defendant conferred with standby counsel)

2   BY MR. SCHULTE:

3   Q. So your conclusion is only one of inference, correct?

4   A. Aside from --

5   Q. You're inferring based on this, right?

6   A. Based on this exhibit and the other stuff I mentioned, yes.

7   Q. What stuff, sir?

8   A. The, like, the testimony from Dave.

9   Q. Those aren't forensics. I'm talking about forensics, sir.

10   What forensics do you have besides this?

11   A. Besides this, I started to say before, we don't have a,

12   like, allow list configuration from the NetApp, like I'd

13   mentioned previously.

14   Q. OK. So you're just inferring based on this, and that could

15   be wrong, right?

16   A. I don't think it's wrong.

17   Q. It could be wrong, right; you don't know?

18   MR. DENTON: Objection.

19   THE COURT: Sustained.

20   Let's move on, Mr. Schulte.

21   MR. SCHULTE: All right. Let's turn to slide 113.

22   Q. Now, your presentation here leaves out a couple of major

23   events at the beginning, does it not?

24   A. I think you're going to have to elaborate.

25   Q. You didn't put on your slide that after the command listing

M6oWsch1   Leedom - Cross

1   files, at 5:29 p.m., the very next command there's a listing of

2   files --

3   MR. DENTON: Objection.

4   THE COURT: Let Mr. Schulte finish the question,

5   please.

6   BY MR. SCHULTE:

7   Q.   -- at 5:55?

8   A.   Can you repeat the question? I'm sorry.

9   Q.   Yeah. So, you didn't put on your slide or you didn't show

10   that after the command listing files at 5:29 p.m., that the

11   very next command is at 5:55 p.m., correct?

12   A.   I'd have to look at the -- like, there is a lot of

13   activity, so what we kind of cut down for the PowerPoint

14   summarizes the, like, the main points.

15   Q.   All right.

16   A.   If you have, like, like a list command at 5:29 and want me

17   to look at it, I'd be happy to look at it, but --

18   THE COURT: Mr. Leedom, just a reminder to slow down.

19   Keep your voice up. Don't swallow your words. Speak, loudly,

20   clearly.

21   THE WITNESS: Yes, sir.

22   MR. SCHULTE: I'm just going to show the witness and

23   the parties something marked defense exhibit 1209.

24   Q.   Now, do you recognize what type of file or what this shows?

25   Do you recognize it?

M6oWsch1   Leedom - Cross

1   A.   Yes.

2   Q.   And it's, you know, it's one of the other types of files

3   that you've exhibited throughout your presentation, right?

4   A.   Yes.

5   MR. SCHULTE: I move to introduce defense exhibit 1209

6   into evidence.

7   MR. DENTON: No objection.

8   THE COURT: Admitted.

9   (Defendant's Exhibit 1209 received in evidence)

10   BY MR. SCHULTE:

11   Q.   And this is a transcript file showing remote access to the

12   ESXi server, correct?

13   A.   This is -- I believe this was recovered from unallocated

14   space on your virt. machine.

15   Q.   It's from the CIA workstation, but it's showing remote

16   access on the ESXi server, right?

17   A.   That's correct.

18   Q.   And it's recording the commands as they're being typed from

19   the workstation, correct?

20   A.   Yes.

21   Q.   OK.   The first command executed here is LS-ALTR, correct;

22   it lists the files?

23   A.   That's correct.

24   Q.   And this is the, you're basing it off the shell log, and

25   it's showing it's 5:29, correct?

M6oWsch1   Leedom - Cross

1   A.   Yes.   If this is the end of the, of the previous command,

2   then yes, that's how I would have time stamped that.

3   Q.   This is right at the beginning of your time line, right?

4   A.   At 5:29?   Yes.

5   Q.   Yeah.

6   All right.   And the very next command is another LS-ALTR,

7   right?

8   A.   Yes, it is.

9   Q.   And this command is 5:55 p.m., correct?

10   A.   Yes, it appears to be.

11   Q.   And this is after the backups are supposedly accessed,

12   right?

13   A.   I believe so.

14   Q.   So between this command at 5:29 and the very next command

15   at 5:55, there are no commands here, right?

16   A.   Not in this exhibit, no.

17   Q.   I mean this is recovered directly from the workstation,

18   right?

19   A.   Yeah, from the unallocated space.   Yes.

20   Q.   OK.   But if there were commands -- well, specifically,

21   there's no command SSH into the Confluence machine, right?

22   A.   No.   We don't have it here in this exhibit.   I'm not sure

23   if it would be in this regardless for that.   But I mean, no,

24   there's no SSH command here.

25   Q.   I mean if the SSH command here was run here, you would see

M6oWsch1   Leedom - Cross

1   it, would you not?

2   A. I'm not sure how exactly, like, how this, like, you called

3   it a transcript, like, how it was, how it came to be. So we

4   got it from deleted space, so --

5   Q. I think we'll go into detail about the transcript file a

6   little bit later, but the point is this is -- you're seeing the

7   output of all, of all the commands that are being executed,

8   correct?

9   A. That's correct.

10   Q. If this, if there was a log-in, or if there was a log-in

11   and commands were being executed on the Confluence system, we

12   would see that here, right?

13   A. We have commands from the OSB server. We don't have

14   commands, like, from the Con -- like, the Ubuntu VM itself.

15   Q. Well, there's no difference between this OSB server and

16   Confluence server; they're both servers, right?

17   A. Well, but this is from a single, like, SSH session.

18   Q. OK. And I mean you -- you show in your presentation, you

19   know, all these events that are occurring during this time

20   frame, right?

21   A. Yes.

22   Q. OK. And specifically, there's no command here to SSH into

23   the Confluence very many, right?

24   A. There's no SSH command from the ESXi server into the

25   Confluence VM.

M6oWsch1   Leedom - Cross

1   Q.   There's no SCP command either, right?

2   A.   Not from this log from the ESXi server.

3   Q.   Well, this is from the CIA workstation. It's from my

4   workstation, right?

5   A.   It is, but it's from a session from the ESXi server.

6   Q.   Showing a remote session into the ESXi server, right?

7   A.   Yes.

8   Q.   But it doesn't show any SCP command, right?

9   A.   No.

10   Q.   And that's the secure copy; that would be what you would

11   run to copy something from the server, right?

12   A.   That's a command you could use to do that.

13   Q.   OK. There's no other copy command that you would run --

14   there's no other copy command either here, right?

15   A.   No, there's not.

16   Q.   OK. In fact, there's no trace of any log-in to the

17   Confluence VM during that reversion period, right?

18   A.   Not in this, in this exhibit, this log, no.

19   Q.   Well, not just this exhibit; all the, all the, all the

20   transcript files that you reviewed, right?

21   A.   Yeah, all the connections from the OSB server, there's --

22   there's, like I said, there's no, like, SSH from the OSB server

23   to the Confluence server.

24   Q.   Well, there's also transcripts from the actual workstation

25   itself, right? The workstation, you have to run a command to

M6oWsch1   Leedom - Cross

1 access the ESXi server, correct?

2 A. Yes, you do.

3 Q. OK. And you testified on direct that these commands don't

4 exist because the Confluence virtual machine was reverted and

5 deleted, right?

6 A. So that's running from the inference that there's --

7 Q. I'm just asking if that's your -- that was your testimony,

8 right?

9 A. Yeah, that's why we don't see, like, a copy command.

10 Q. But of course, reverting or deleting the Confluence virtual

11 machine has absolutely no effect on transcript files from my

12 own CIA workstation, correct?

13 A. That's correct. If we're calling those -- the exhibits of

14 all the commands, if that's what we're calling transcript

15 files, we can call them that.

16 Q. OK.

17 A. I can't determine, you know, exactly what their source is

18 there, but --

19 Q. We'll get into that later, but -- so your testimony then

20 from direct is not correct, right? Your testimony that you

21 said you don't, these commands don't exist because the

22 Confluence virtual machine was reverted and deleted, that

23 testimony is wrong, right?

24 A. No.

25 Q. You just said, you disagreed that reverting or deleting the

M6oWsch1   Leedom - Cross

1   Confluence virtual machine has no effect on the transcript

2   files from my own CIA workstation, right?

3   A.   Assuming that -- figuring, that there is transcript file

4   for that activity in the first place. What I testified to on

5   direct was that there's no copy command -- in my opinion, the

6   copy command would be in that Confluence virtual machine,

7   should be on the virtual machine there, and that's where you'd

8   be running, running those commands from.

9   Q.   I mean, you don't have to -- you could run the commands

10   from anywhere; you don't have to log in to the Confluence

11   machine to run the copy command, right?

12   A.   You could use SCP, which you would have to -- I mean that

13   does have to log in to the machine to do that.

14   Q.   Right.

15   A.   So the logs of that log-in would be on the VM, which were

16   deleted. That's what I'm testifying to, is that any activity

17   that would have affected files connected to that Confluence

18   virtual machine was deleted. So, you know, that could be a

19   copy command. That could be an SCP session to copy to the

20   network that's authenticating, things like that.

21   (Continued on next page)

22

23

24

25

M6o5sch2   Leedom - Cross

1   BY MR. SCHULTE:

2   Q. So your testimony is the logs on Confluence are no longer

3   available, right?

4   A. That's correct.

5   Q. But any transcript file or any log from my work station

6   would still be available, right?

7   A. I wouldn't say any. I don't know these circumstances

8   around what makes the transcripts when they're there, what

9   turned them on and off, things like that, but all I can really

10 speak to is the evidence that's here about all the activity on

11 the ESXi server itself and I think, like you said, there is

12 some from the -- from the VM itself.

13 Q. I mean, if we look at this, you know, this was -- if this

14 was a server, a virtual server and it was reverted, these files

15 would remain on my work station, right?

16 A. Yes, because it came from your virtual machine.

17 Q. So the point is anything that you do to another server or

18 another system is not going to affect logs or documents being

19 produced on this work station, right?

20 A. That's correct.

21 Q. OK. Essentially since the source of these transcript files

22 is my CIA work station, they are preserved no matter any

23 snapshot or reversion, right?

24 A. Correct.

25 Q. And if I logged in here, or if I ran an SCP command here,

M6o5sch2   Leedom - Cross

1   you would see the transcript files on the CIA work station just

2   like you do the ESXi server, right?

3   A.   I mean, I can only speak to what we recovered so we didn't

4   recover any commands like that.

5   Q.   So I think your testimony though, on direct, was that these

6   commands would not be here at all, correct?

7   A.   Like I said before, my testimony is about the actual

8   Confluence, like virtual machine itself, and those logs which

9   were deleted from the snapshot reversion, not that there, you

10   know, could be commands in a transcript that was missing and

11   not being able to be recovered from your work station.

12   Q.   OK. So your testimony is specifically just about any logs

13   that were on Confluence, right?

14   A.   Yes, specifically to, like, copy command, that kind of

15   thing; yes, that is correct.

16   Q.   But as for the transcript files, unallocated space, and my

17   work station, you looked everywhere there for a copy command

18   during the reversion; correct?

19   A.   Yes. I searched through it for alt commands, not just

20   copy, but.

21   Q.   You were really looking for copy commands, right?

22   A.   I mean, sure. Copy commands, like I said, any commands are

23   really valuable so it is not like I searched only for copy

24   commands.

25   Q.   You really scrutinized the work station over the last five

M6o5sch2   Leedom - Cross

1 years, right?

2 A. Not like every day over the last five years but, yes, it

3 was reviewed in some time in the last five years.

4 Q. You did a complete forensic analysis on the work station,

5 right?

6 A. That's correct.

7 Q. You looked for a copy command during the reversion period,

8 right?

9 A. Yes.

10 Q. Looked high and low, right?

11 A. That's correct.

12 Q. You did not find a copy command during the reversion,

13 correct?

14 A. No.

15 Q. You did not find any logins to the Confluence virtual

16 machine during the reversion, correct?

17 A. No, not that I believe.

18 Q. And you know all these very specific times on your timeline

19 from the transcript files, right?

20 A. There are still estimates, I would call them very specific

21 estimates, but yes.

22 Q. I mean, the point is there is no -- there is no files that

23 were deleted or activity that was executed that is not -- that

24 you didn't find transcript files for, right?

25 A. Included in the timeline here as far as everything on the

M6o5sch2   Leedom - Cross

1   bottom? Everything on the bottom here comes from transcript

2   files aside from the vault stuff.

3   Q. If you hire a painter to paint a room, how many times do

4   you have to check the room to know he didn't paint it yet?

5   MR. DENTON: Objection.

6   THE COURT: Sustained.

7   Q. OK. Once and for all, forensically, based upon only your

8   forensic findings, can you say that I copied the March 3rd,

9   2016 Confluence backup on April 20th, 2016?

10   A. There is no copy command, like, attributable to you for

11   that.

12   Q. Just the forensics, based on your forensic findings?

13   A. I think taking them all together is part of the finding but

14   there is no, like -- we don't have a forensic artifact of a

15   copy command for that.

16   Q. Back to the logs. You have all -- again, you have all the

17   logs from the CIA work station, right? From my CIA work

18   station?

19   A. That we were able to recover, yes.

20   Q. You testified they're all in tact, right? There were no

21   deletions of those files, right?

22   A. Yes. On the host I don't recall seeing like any evidence

23   of deletion.

24   Q. And this includes logs of removable media, correct?

25   A. Yes.

M6o5sch2   Leedom - Cross

1   Q. You have the logs for every device I ever connected into

2   the CIA work station for how long, right?

3   A. Yes, in a general sense.

4   Q. And you also recovered every single device I connected into

5   the CIA work station, right?

6   A. I don't remember from, like, an inventory perspective. I

7   don't remember.

8   Q. During the reversion period there are no removable media

9   connected to my CIA work station, correct?

10   A. I don't believe so. I don't think there was artifact of

11   that. I know there was one that was connected, like, recently,

12   the one that was connected to a write blocker, but I think that

13   was -- that might have been on the 18th. Maybe. I don't quite

14   remember the date for that but no to my knowledge I don't

15   believe there was a USB artifact from during the reversion

16   period from your work station.

17   Q. If there had been one you would have put it in your

18   presentation, right?

19   A. Yes.

20   Q. It would have been important that removal media or large

21   hard drive was being plugged in, right?

22   A. Yes. That would be important.

23   Q. And there are no forensic artifacts showing any of the

24   Atlassian backups copied to my CIA work station, right?

25   A. No.

M6o5sch2   Leedom - Cross

1   Q. In fact, the virtual machine was only 50 gigabytes, right?

2   A. I don't remember the exact size.

3   Q. You don't remember the exact size?

4   A. No.

5   Q. But in any case, there is no -- you have the unallocated

6   space and you have all the forensic artifacts that you are able

7   to find like link files and open files, all this forensic

8   evidence that you went through and there was no evidence of any

9   backups on the computer, right?

10   A. No, not on your work station.

11   Q. There are no forensic artifacts showing any of the

12   Atlassian backups were ever copied to any devices I possessed

13   or used at the CIA, correct?

14   A. Not to my knowledge.

15   Q. In fact, you never even suggest through your whole

16   150-slide show, you never present a theory for a copy, correct?

17   A. I think I did present the theory for the copy in that it

18   happened during the reversion period on the Confluence virtual

19   machine, but.

20   Q. I mean, without any removal media connected to my CIA work

21   station during the reversion it is not possible to steal the

22   backups, is it?

23   A. I mean, there is attached network shares, there is other

24   ways than just removal media. You could stage the data or move

25   it.

M6o5sch2   Leedom - Cross

1 Q. I mean, you found no evidence of any of that though, right?

2 A. I don't have a whole lot of visibility for some of that.

3   THE COURT: Can you explain what you mean by attached

4 network share?

5   THE WITNESS: Yes. So like we saw, as an example,

6 like the home folders, that's all connected over the network to

7 the various work stations so, like, that could be a potential

8 location something could be copied to. It doesn't necessarily

9 have to be copied straight to the machine.

10   MR. SCHULTE: Object.

11 BY MR. SCHULTE:

12 Q. All right. The point is, though, your review of -- you had

13 the whole DevLAN network and on your review of all these

14 systems you didn't find copies to those, right?

15 A. Not to my -- not that I remember, like a -- but -- go

16 ahead.

17 Q. You would have, from the CIA work station if there was

18 mounted directories or mounted network shares, you would have

19 seen logs of those; right?

20 A. I think most work stations had, like, home folder, those

21 basic shares that we looked at mounted already so it is not

22 like you have to make a new mount, but.

23 Q. So what exactly is the working theory of how this data was

24 copied?

25 A. That it was copied during the reversion period from the

M6o5sch2   Leedom - Cross

1   Confluence VM.

2   Q. But again, you said there is no forensic artifacts of those

3   copies, right?

4   A. No, because you deleted all of the locations where --

5   Q. Again, you are talking about the Confluence system. There

6   is no deletions from my -- from my logs, right?

7   A. I mean, from what we were able -- there is no -- what do

8   you call it -- like copy commands from your virtual machine

9   from what we recovered, no.

10   Q. OK. So -- and again, with no removable devices connected,

11   no logs that you have shown of network shares or copies to

12   network shares -- I am struggling to see what would have the

13   Confluence backups have been copied to?

14   A. So like I said, it could have been copied to a network

15   location. I mean, it's tough in general because when we

16   arrived on site it was a year afterwards and, like, we have

17   spoken to the availability of network logs and some of those

18   things are just not available. So, like, from all the evidence

19   retrieved and everything that is there, this is how I put my

20   theory together.

21   Q. But from my work station, again, the logs are all in tact

22   there and there is nothing in those logs, right?

23   A. From the host? No.

24   Q. And you keep saying could have been copied. You see no

25   forensic evidence of that, right?

M6o5sch2   Leedom - Cross

1 A. Not from --

2   THE COURT: I think we have trod this ground plenty.

3 Move on, please.

4 BY MR. SCHULTE:

5 Q. You testified it was possible to copy the backup files in

6 an hour, right?

7 A. Yes.

8 Q. And your presentation slides do not show the forensic basis

9 for your conclusion, right?

10 A. No, there is no --

11 Q. OK. You did not establish network speed, right?

12 A. I'm sorry?

13 Q. In your slides you don't establish network speed, right?

14 A. No.

15 Q. You don't address the variables that degrade the network

16 speed, right?

17 A. No, not in my network slides.

18 Q. A forensic expert cannot validate your claims, right?

19 A. Can you explain?

20 Q. Yes. A forensic expert has no idea what test you

21 performed, right?

22 A. I think those tests might have been in my notes.

23 Q. I'm talking about your presentation, sir.

24 A. Oh no.

25 Q. Based upon your presentation a forensic expert cannot

M6o5sch2   Leedom - Cross

1   validate any of your claims, right?

2   THE COURT: Sustained.

3   Q. Again, the forensic expert does not know what tests you

4   performed, correct?

5   A. I disagree. I don't remember if they're in my notes or

6   not.

7   MR. DENTON: Objection.

8   THE COURT: One at a time, and sustained. Let's ask a

9   new question, please.

10   BY MR. SCHULTE:

11   Q. Your presentation -- in your presentation it does not

12   reflect any tests you performed for network speed, right?

13   A. That's correct.

14   Q. In fact, there is nothing through your presentation for a

15   forensic expert to analyze, all they know is your conclusion,

16   they don't know your analysis at all, right?

17   MR. DENTON: Objection.

18   THE COURT: Sustained.

19   BY MR. SCHULTE:

20   Q. Take a look at your presentation. Can you show me where

21   you analyze this?

22   MR. DENTON: Objection.

23   THE COURT: Sustained.

24   Q. The fact that you do not even have a theory as to what

25   device the data was copied to, this also impacts your analysis,

1   correct?

2   A. Can you define "impacts my analysis?" What do you mean by

3   that?

4   Q. Yeah, sure. A theory of splitting the backup files across

5   multiple drives or using slower drives obviously impacts the

6   analysis, correct?

7   MR. DENTON: Objection.

8   THE COURT: Overruled.

9   A. To some extent it impacts the conclusion just because I

10   would say I don't have the, like, an exhibit for that. To the

11   extent I don't have an exhibit that affects my analysis, yes.

12   Q. Without knowing precisely what device or where information

13   was copied, you can't say how long it would have taken, right?

14   A. Oh, I don't know, I disagree.

15   Q. You disagree? You can theorize how long something takes to

16   copy without specifying what it is being copied to?

17   A.   I think if it was taken -- so like the tests that I ran

18   were based on copying to, like, a network location or just the

19   file transferring of the network in general, so whether it was,

20   like, copied somewhere quickly and, like, staged and copied

21   later or something like that, I can't say, obviously, like I

22   don't have a log of a certain USB device or a certain firmware

23   number that I could test. No, I don't have that.

24   Q.   I mean, if it is being copied to a tape drive it is going

25   to take a long time to copy, right?

M6o5sch2   Leedom - Cross

1   A.   If it was being copied to a tape drive it would take longer

2   than being copied to, like, a solid state drive. On a matter

3   of principle, yes.

4   Q.   Or how much data is being copied depends on your analysis

5   too, right?

6   A.   To some extent. I don't know exactly what you are getting

7   at but I can say my copy estimate was based on the total size

8   of Stash and the total size of the Confluence backups and, yes,

9   it was very possible, in an hour time frame, more than enough

10   to copy it.

11   Q.   Based on the configuration of Deadline alone it would have

12   taken at least four hours, correct?

13   A.   I can't speak to that.

14   Q.   Let's say at a speed of 100 megabits per second it would

15   have taken four hours to copy 200 gigabytes?

16   A.   Why would it only be 100 megabits?

17   Q.   No, that's not the question.

18   A.   Are you asking, like, from a mathematical standpoint?

19   Q.   Yes.

20   A.   Can you give me the numbers again?

21   Q.   At 100 megabits per second it would take four hours to copy

22   200 gigabytes, correct?

23   A.   It sounds close. I would want to run it through a

24   calculator probably but that sounds somewhat close.

25   Q.   I mean, we can walk through the math.

M6o5sch2   Leedom - Cross

1   MR. DENTON: Objection, your Honor.

2   THE COURT: Sustained.

3   Q. So you said something about -- well, OK. Let's move on to

4   the backups. It is fair to say that you don't know what DevLAN

5   files WikiLeaks currently possesses, right?

6   A. No. I disagree.

7   Q. You have a contact in WikiLeaks?

8   A. No.

9   MR. DENTON: Objection.

10   THE COURT: Sustained.

11   Q. How do you know what files WikiLeaks has?

12   A. I mean I showed my presentation, the reasons why I believe

13   that they have that March 3rd backup.

14   Q. You believe. You don't know, right?

15   A. Did you ask me if I believed? Yes.

16   Q. It is fair to say you don't know what DevLAN files

17   WikiLeaks currently possesses, right?

18   A. Like I said, I have what I have presented. I don't have

19   like a, you know, transcript from them saying this is the file

20   we have but, I mean, there has been a lot of review done to

21   show why that is the -- that is the backup file that was

22   posted.

23   Q. I mean, all you know is what WikiLeaks was disclosed,

24   right? That's all you know?

25   A. That's correct.

M6o5sch2   Leedom - Cross

1   Q. So WikiLeaks could have files that you don't know about,

2   right?

3   A. They could have all kinds of things, I'm sure.

4   Q. But based on the WikiLeaks disclosure, you know that at the

5   very least they must have a copy of both Stash and Confluence,

6   right?

7   A. Yes, and I don't know if it would need to be the entire

8   Stash backups because I don't believe -- of the products

9   released there were a handful of products released.

10   Q. Again, that's because you don't know what WikiLeaks has,

11   right?

12   A. No, I don't have it. Like I said, I don't have a log of

13   the exact files they have, just from the analysis of the, like,

14   timelining of what backups are available, where things could

15   have come from, and the points I made in the presentation.

16   Q. Just to be clear, the Stash and Confluence backups, they're

17   digital files, right?

18   A. Yes.

19   Q. They're intangible, correct?

20   A. Intangible? Like, what do you mean by that?

21   Q. They're not tangible, hard copy documents; correct?

22   A. They're -- I mean, put them on a hard drive. Is that

23   tangible? They're digital files.

24   Q. And you conducted an examination of the Stash, Confluence,

25   and other Atlassian products' backups on DevLAN, right?

M6o5sch2   Leedom – Cross

1   A.   Yes.

2   Q.   You are familiar with version control, right?

3   A.   Yes.

4   Q.   Version control literally keeps track of the edits or

5   reversions of a file, right?

6   A.   Yes.

7   Q.   You are familiar with Git, right?

8   A.   Yes.

9   Q.   And Git is just a form of version control, right?

10   A.   Yes, it is.

11   Q.   And the Atlassian backups were essentially generated by

12   simply copying all the data from the server into a single file,

13   right?

14   A.   Two files.

15   Q.   Two files; a SQL file and the compressed file, right?

16   A.   Correct.

17   Q.   The TGZ file is the compressed file, right?

18   A.   Yes.

19   Q.   The compression is simply a way to reduce the file size

20   without losing data, right?

21   A.   That's correct.

22   Q.   When the underlying Atlassian data from the servers is

23   modified or deleted, a record of those changes is created,

24   correct?

25   A.   Yes; in the database.

M6o5sch2   Leedom - Cross

1   Q. This allows a user to review all the changes over time,

2   right?

3   A. For the most part, yes.

4   Q. This is sort of like tracked changes in Microsoft Word or

5   in Google Docs, correct?

6   A. Yes.

7   Q. The user essentially has access to all prior versions of

8   the data, right?

9   A. I believe so.

10   Q. And each successive backup contains the data of all the

11   prior backups, right?

12   A. To some extent.

13   Q. There is some data that's not maintained through Git?

14   A. Are you talking about Stash or Confluence? They're kind of

15   different.

16   Q. Well, both.

17   A. So I mean, like, using Git as an example you can definitely

18   remove stuff from Git, like, prior commit history as an

19   example. For Confluence I believe, like I showed in my

20   presentation, if a page is deleted, that can be in the database

21   still and be like marked as deleted.

22   Q. So all the data that was released by WikiLeaks can be found

23   in every single backup starting with the March 3rd, 2016 backup

24   all the way through the March 6, 2017 backup, right?

25   A. Is that like the most recent one that was in there?

M6o5sch2   Leedom - Cross

1   Q.   Well, I'm saying WikiLeaks released the data March 7, 2017,

2   right? So the backup before that would contain the data as

3   well, right?

4   A.   I didn't do, like, the timeline, so I'm not sure exactly

5   for that, like, that backup specifically. Like I said, you can

6   change files in there, it is possible.

7   Q.   Yeah. The question is just that the data released by

8   WikiLeaks is found in all the backups from March 3rd, 2016 to

9   March 6, 2017, right?

10 A.   Sitting here today I'm not sure. It has been a long time

11 since I looked at all of those but, like, from a general

12 standpoint, they are version controlled so if you removed a

13 page it would still be removed unless you unremoved it later.

14 Stuff can change.

15 Q.   Due to the version control feature the backups are going to

16 contain all the data preceding it?

17 A.   In a general sense.

18 Q.   So if WikiLeaks received the March 6, 2017 backup file they

19 had a choice of which one of the versions prior to the March 6

20 version they could release, right?

21 A.   I disagree. I think it is a lot more complicated than just

22 picking a date and saying revert the whole thing to this one

23 date.

24 Q.   I mean, you are familiar with Git, you said, right?

25 A.   I think I really need to separate the Stash from the

M6o5sch2   Leedom - Cross

1   Confluence because they do operate very differently from a

2   technical standpoint.

3   Q. So for the Stash files it would have been trivial to do

4   through Git, right?

5   A. It depends on what's there. Like I said, I didn't do a lot

6   of the timing analysis for Stash, I focused more on Confluence.

7   I probably did more Stash side of the house.

8   Q. I am talking about the Stash backups are based on Git,

9   right?

10 A. That's correct.

11 Q. And you have knowledge in Git, right?

12 A. Yes.

13 Q. So if you have a commit log from Git all the way to March

14 7, 2017, right?

15 A. Assuming it is in tact and wasn't ever edited.

16 Q. OK, you could go back and select the commit from March 3rd?

17 A. You could. If it was there, yes, you could go back and --

18 Q. And Git makes this trivial to do, right?

19 A. It is easy to do.

20 Q. You testified that it may take some time to do this for

21 Confluence, right?

22 A. Yes.

23 Q. And you also testified that sifting through the corrupt

24 database would have also taken a lot of time, right?

25 A. Yeah. From my experience working with it, yes, it would

1   have.

2   Q. And according to you, WikiLeaks spent the time to retrieve

3   content from the corrupt database, correct?

4   A. Yes.

5   Q. They exerted that effort to do so, right?

6   A. It appears so. From what they posted and what is in the

7   database, yes.

8   Q. And from your investigation you learned about WikiLeaks,

9   right?

10   A. Can you elaborate?

11   Q. I mean --

12   A. Like in a general sense?

13   Q. Yeah.

14   A. Yes.

15   Q. You learned, did you not, that WikiLeaks limits its release

16   of data to protect its sources, right?

17   MR. DENTON: Objection.

18   THE COURT: Sustained.

19   Q. As part of your investigation you wanted to learn how

20   WikiLeaks released its information, right?

21   A. I mean, I have a general sense of what they posted in the

22   past.

23   Q. You made an effort to learn how they did this in the past,

24   right?

25   A. Yes, from -- just from reviewing, like, previous releases.

M6o5sch2   Leedom - Cross

1   Q.   And these releases would show you that WikiLeaks limits its

2   release of data to protect its source, right?

3   MR. DENTON: Objection.

4   THE COURT: Sustained.

5   Q.   I want to talk to you now about the CIA's offsite backup.

6   Backups from the Altabackup server were regularly taken off

7   DevLAN and moved to an offsite backup, correct?

8   A.   From what I understand, yes.

9   Q.   All the backups were stored at the offsite backup, right?

10   A.   The offsite backups were stored there, yes.

11   Q.   And it is possible that WikiLeaks received the backup file

12   from the CIA's offsite backup, correct?

13   A.   I disagree.

14   Q.   All right. Well, let's pull up what is in evidence as

15   Government Exhibit 602 and this is page 2 of the document. Do

16   you see the offsite backup site?

17   A.   Yes.

18   Q.   WMA storage; right?

19   A.   Yes.

20   Q.   Backups from the Altabackup server were regularly taken off

21   DevLAN and moved to the offsite backup, right?

22   A.   Yes.

23   Q.   Did you conduct a forensic examination of the offsite

24   backup?

25   A.   Yeah, we had a -- I think we had a copy of that as well.

M6o5sch2   Leedom - Cross

1   Q.   No.   Did you conduct a forensic examination of the site?

2   A.   I have never been to the site.

3   Q.   So no.

4   A.   I can't really speak to the collection at the site because

5   I didn't, like there is a cart -- the FBI forensics thing. I

6   know that, like, reviewing, like, I had access to review the

7   data stored from there but as far as specific questions for

8   seizures, things like that at the site, physical stuff, I can't

9   really speak to.

10   Q.   So I mean, if someone stole the backup from the offsite

11   backup and leaked them to WikiLeaks, you would have no

12   knowledge of that, right?

13   A.   I disagree; just from the -- I do know the security

14   controls for the site and the fact that I think it was, like, a

15   one-way transfer from, like, from DevLAN to the site and I --

16   Q.   I'm not asking about someone from DevLAN, I am specifically

17   asking about the offsite backup. If somebody stole the backups

18   from the offsite backup and leaked them to WikiLeaks, you would

19   not have any knowledge of that, right?

20   A.   I mean, we have the like same file access time information

21   from the main site that we do from the Altabackup share --

22   sorry, the offsite backup. So if those files were copied, that

23   metadata would be changed in the same way that it is in what we

24   have showed in the presentation so that's how I would determine

25   whether something was copied there.

M6o5sch2   Leedom - Cross

1   Q. You don't present any of that in your presentation though,

2   right?

3   A. No. From what I understand it either, like, was an

4   identical match to the data that we had or there wasn't any

5   evidence of that type of thing over there.

6   Q. Would your analysis be any different if the backups were

7   taken from the offsite backup?

8   A. If I was showing -- I would be showing something kind of

9   similarly, like maybe an access time but I don't remember,

10   honestly -- six years later now -- I don't remember the exact

11   security requirements for accessing that site. I don't know if

12   you could even, like, access the files that were there without

13   physically being there. I don't remember.

14   Q. What about do you know if WikiLeaks received the backup

15   file taken from COG through Hickok here?

16   A. I mean, it is my opinion that didn't happen.

17   Q. OK. Let's take a look at your presentation on page 11, and

18   you can see here, like, on the other page Jira is connected to

19   Hickok, right?

20   A. Yes.

21   Q. And you investigated the Hickok-Jira connection with COG,

22   right?

23   A. To the extent, like I have reviewed the security plans for

24   the firewalls that are in place there. The server itself, I

25   don't know if it was re-purposed.

M6o5sch2   Leedom - Cross

1   Q. So you reviewed technical documents about how it should

2   have run?

3   A. That's correct.

4   Q. So DevLAN connected to the COG network here, right?

5   A. I don't see your cursor but if you are talking about the

6   little bricks and the --

7   Q. Yes.

8   A. Yes.

9   Q. So if we can pull up Government Exhibit 601, which is also

10   in evidence, this is describing the fire walls there, right?

11   A. Yes. This is one of the documents that describes them.

12   Q. Can you read the first, just that line there?

13   A. The confidential marked line?

14   Q. Yes.

15   A. The only traffic allowed into and from Hickok is HTTPS,

16   SLDAP, SMTP, and SSH.

17   Q. Do you see that Hickok is set up to ensure SSH access;

18   right?

19   A. Yes, but from only one side.

20   Q. SSH is a way to remotely access another computer, right?

21   A. Yes.

22   Q. Hickok permits SSH access, correct?

23   A. The firewall rules permit it. Like I said, I don't know

24   about, like, if there were -- what was configured on the server

25   specifically. I don't have a -- I don't have, like, the logs

M6o5sch2   Leedom - Cross

1   from the server itself but from the firewall configuration,

2   yes, SSH was allowed from either netware to the server.

3   Q.   So someone from DevLAN can SSH into Jira, correct?

4   A.   Yes.   That's what I understand.

5   Q.   And someone from COG can SSH into Jira too, right?

6   A.   That's what I understand.

7   Q.   And Jira mounts the Altabackups, correct?

8   A.   So I believe so. The only issue is, like, NFS or, like,

9   CIFS or --

10   Q.   I am just asking if Jira mounts the Altabackups.

11   A.   I know there are backups from Jira in Altabackup.

12   Q.   And it needs access to Altabackups so it can store the Jira

13   backups, right?

14   A.   You can technically, like, SSH in and move them down. I

15   don't know the frequency of the backups from Jira, I don't

16   recall at this time so I don't know if it was something that

17   were moved down over SSH or if it was set up in the same

18   automated way that the other services were set up. I just

19   don't recall at this point.

20   Q.   Would Jira connect directly to the Altabackup server,

21   right?

22   A.   I can't say. Other than the fact that there are backups

23   from Jira there I can't say the exact connection.

24   Q.   Those backups are created -- their creation access and

25   modified times show that they're being created and stored there

M6o5sch2   Leedom - Cross

1   live, right?

2   A.   Like I said, I don't know if they were, like, daily or if

3   they were pushed in batches. I haven't looked at them in a

4   while -- Jira backups anyway.

5   Q.   So someone who logs into Jira could also then access the

6   backups, correct?

7   A.   If Altabackup was mounted, then theoretically yes.

8   Q.   Someone from COG need only to SSH into Jira to access and

9   copy the backup files, right?

10   A.   If it was mounted. I can't speak to the exact state of it

11   other than I know there were backups from Jira on Altabackup.

12   Based on the firewall configs, like, NFS isn't explicitly

13   allowed here so that presents an issue, but.

14   Q.   I mean, you reviewed the Jira server, right?

15   A.   Like I said, I think that server might have been

16   re-purposed. I don't believe I have, like any -- I don't think

17   I have any logs or anything from the Hickok server.

18   Q.   But based on the directory Altabackup -- the Jira folder

19   and the Altabackup directly, the fact that these files were

20   being written there and from my work station it seems to

21   indicate that this is the case, right?

22   MR. DENTON: Objection.

23   THE COURT: Sustained.

24   Q.   You reviewed my CIA work station, right?

25   A.   Yes.

M6o5sch2   Leedom - Cross

1   Q. You could see the logins to Jira, right?

2   A. There is an attempt I know, at least on 4-18 to log into

3   Jira.

4   Q. Before that you know there were successful logins to Jira?

5   A. I believe so.

6   Q. And in the history files there there were -- it showed that

7   the Jira mounted Altabackups, right?

8   A. I don't remember.

9   Q. In COG there is at least the same -- at least 200 people

10   working COG, right?

11   MR. DENTON: Objection.

12   THE COURT: Sustained.

13   Q. Well, the individuals working in COG were experienced in

14   using the malware tools, correct?

15   MR. DENTON: Objection.

16   THE COURT: Sustained.

17   Q. Are you familiar with what COG is?

18   A. Only so much that it's an operations group. I don't

19   know -- I can't speak to their expertise or training.

20   Q. OK, but EDG writes the malware and sends it to COG to use

21   it, right?

22   A. I know they are the customer for those tools.

23   Q. Nowhere in your presentation is there any slide about the

24   investigation to access to the Jira server, correct?

25   A. No.

M6o5sch2   Leedom - Cross

1   Q. Did you conduct any analysis of COG's network?

2   A. I did not personally, no.

3   Q. Did anybody?

4   A. I can't speak to anybody. I don't -- I know at least for

5   myself I think the Bureau, I don't believe it was investigated.

6   Q. And why was it not investigated?

7   MR. DENTON: Objection.

8   THE COURT: Sustained.

9   Q. Based on your forensic knowledge of the way the systems

10 were set up, COG could have access to the Altabackup server,

11 right?

12 A. I disagree from the -- it's hard for me to say without

13 having reviewed Hickok and the logs. All I can really speak to

14 is the configurations, like, since I can't confirm the mount

15 for Altabackup on the time. I know that those backups were

16 there. Whether they were there over NFS from the share or

17 whether they were, like, moved down over SSH is kind of all I

18 can really speak to. If it was mounted to Altabackup and you

19 could SSH into it, then.

20 Q. I mean, even if it was moved -- you keep saying if it was

21 moved down through SSH, right? If it is moved down through SSH

22 that is somebody actually running a copy command from Jira to

23 copy those, right?

24 A. If you did it like that you would only have access to the

25 backups that were like currently staged on the Jira server

M6o5sch2   Leedom - Cross

1   itself, not all of everything in Altabackup.

2   Q. You are writing -- if you are copying files from Jira to

3   Altabackup you have write access, right?

4   A. Well, you -- so, yeah, but you wouldn't be able to mount it

5   over NFS if it was blocked at the firewall. That's the point

6   I'm trying to make.

7   Q. Yes, but the firewall -- If the firewall is allowing SSH

8   and Jira is mounting the directory and that's available to

9   someone from COG, you could take those files, right?

10   MR. DENTON: Objection.

11   THE COURT: Sustained.

12   Q. So I guess your testimony is essentially you don't remember

13   or you don't know anything about the Jira setup?

14   A. Aside from what we just reviewed and the Jira backups that

15   there are some Jira backups, I can't speak to the server

16   configuration.

17   Q. That server configuration would have been very important in

18   your forensic examination, right?

19   A. Yes.

20   Q. And you don't remember anything about it now?

21   A. No.

22   Q. OK. Let's pull back up Government Exhibit 602. There is

23   also two foreign offices that are connected to EDG, right? To

24   DevLAN?

25   A. Yes, from what I understand.

M6o5sch2   Leedom - Cross

1   Q.   Each of the foreign offices has a system that's connected

2   to DevLAN, right?

3   A.   I can't speak to the configuration. I know we received

4   evidence from the foreign offices. That's really the extent of

5   the foreign offices that I can speak to.

6   Q.   This connection is established over the Internet, right?

7   A.   I don't know, I can't -- I can't speak to the actual, like,

8   network connection.

9   Q.   You did not conduct a forensic examination of the system in

10   the foreign office?

11   A.   The work station? It was connected to DevLAN.

12   Q.   You are saying that you don't know how this -- how it was

13   configured?

14   A.   I don't know how the networking configuration from DevLAN

15   to the foreign office is set up. I just know that -- and from

16   what I have been told and what we received from evidence from

17   the office that there were some workstations connected to

18   DevLAN from the location.

19   Q.   So you don't know if this -- these connections were

20   misconfigured or otherwise insecure, right?

21   A.   I can't speak to the actual connection.

22   Q.   It is fair to say that both adversary and friendly nations

23   run cyber operations against each other; right?

24   MR. DENTON: Objection.

25   THE COURT: Overruled.

M6o5sch2   Leedom - Cross

1   If you know.

2   THE WITNESS: In a general sense, yes.

3   BY MR. SCHULTE:

4   Q. And do you know that the United States has friendly nations

5   and adversary nations, right?

6   A. I can't really speak to our foreign policy.

7   Q. I mean, do you know that adversaries to the United States

8   try cyber operations against the United States?

9   A. Yeah. In a general sense, yes.

10   Q. And it is not unreasonable to think a foreign intelligence

11   service might want access to DevLAN, correct?

12   A. DevLAN or other classified networks I'm sure.

13   Q. So if they breached DevLAN through these connections they

14   would have the ability to copy the backups, right?

15   A. I can't really speak to that.

16   Q. You can't speak to the fact if they are able to breach

17   DevLAN whether they would have access to information on DevLAN?

18   A. Well, I can't speak to the -- I don't know how anything

19   about how that connection was set up, so.

20   Q. The question is if they were able to reach DevLAN would

21   they have been able to copy the backups.

22   MR. DENTON: Objection.

23   THE COURT: Overruled.

24   A. So they would have the same type of, like, user access. It

25   is a really theoretical question because at what level did they

M6o5sch2   Leedom - Cross

1   breach it? Like, with what permissions? There is kind of a

2   lot of open questions.

3   Q. Essentially you don't know -- since you don't know how the

4   connections are set up you don't know if a breach is possible

5   or what kind of access they would have, right?

6   A. No, not from that, from, like, the foreign office link I

7   can't speak to it. I don't know the --

8   Q. OK. Let's move on to the home directories of the

9   Altabackup server, Government's Exhibits in evidence 1207-60

10   through 63. This is the home directories, right, from DevLAN?

11   A. Yes.

12   Q. That's what all these exhibits are, right? Same thing?

13   A. Yes, same; home folders for users.

14   Q. I am going to show to the parties what's been marked as

15   Defendant's Exhibit 1201. Do you recognize what this is?

16   A. Yes.

17   Q. And this is a document from -- showing information about

18   DevLAN, right?

19   A. Yes, for the -- showing information about the file server.

20   MR. SCHULTE: I move to introduce 1201 into evidence.

21   MR. DENTON: No objection.

22   THE COURT: It is admitted.

23   (Defendant's Exhibit 1201 received in evidence)

24   BY MR. SCHULTE:

25   Q. So this is a listing of the shares on the Altabackup

1   server, correct?

2   A.   I -- this is some of the shares.   Like, I don't think

3   Altabackup is in here because this is just the CIFS --

4   C-I-F-S -- shares.

5   Q.   On the second page do you see where it says the "share

6   name: Home"?

7   A.   Yes.

8   Q.   And the "group name: Everyone"?

9   A.   Yes.

10   Q.   What permissions does it give everyone?

11   A.   Full control.

12   Q.   What does full control mean?

13   A.   You can create files, delete files, open files. Pretty

14   much everything.

15   Q.   So the DevLAN home directories were set up publically,

16   right?

17   A.   Home folder, yes.

18   Q.   Anyone could copy files to each other's home directories,

19   right?

20   A.   I don't remember, like, the exact details. I remember

21   hearing about that but I don't know how regular an occurrence

22   it was.

23   Q.   Through your investigation you learned developers regularly

24   used this as a mail transport service with each other to

25   transport data, right?

1   MR. DENTON: Objection.

2   THE COURT: Sustained.

3   Q. Were you able to review what kinds of documents were stored

4   on the home directories?

5   A. Yes.

6   Q. Based on those files, was it clear to you that this home

7   directory is used as a transport?

8   A. I don't know if I call it a transport. I mean, people had

9   this as storage for people to put their stuff. Yes, everyone

10 could access it.

11 Q. So if you are on DevLAN and you want to send files to

12 someone else, you can copy them to his share or you can say

13 *Look at my share*. Right?

14 A. Yeah. With the permissions, you could do that.

15 Q. And we spoke very briefly about Dave C. and his lost drive,

16 right?

17 A. Yes.

18 Q. Dave C. also stored a copy of Stash, the CIA's crown

19 jewels, on his public home directory, correct?

20   MR. DENTON: Objection to form.

21   THE COURT: Sustained.

22 Q. Dave C. stored a copy of Stash on his public home

23 directory, correct?

24 A. Yes. I believe there was a copy of Stash in Dave's home

25 folder.

M6o5sch2   Leedom - Cross

1   Q. And that's admitted exhibit 1207-85? This is a copy of

2   Dave's home directory, right?

3   A. Yes.

4   Q. And you see the folder titled: Stash backup 4/16/16?

5   A. Yes.

6   Q. This is what is in the other directory, this is just named

7   Stash, right?

8   A. It appears so.

9   Q. It is the SQL database?

10   A. Yes.

11   Q. I'm sorry 1207-86 in evidence.

12   And 1207-87 is also in evidence and this is the Stash

13   backup, the 4/16-16 directory; right?

14   A. Yes.

15   Q. And that's Dave's directory, right?

16   A. Yes.

17   Q. And this is a full copy of the entire Stash data, correct?

18   A. It appears to be the correct size.

19   Q. The data released by WikiLeaks is contained in this file,

20   correct?

21   A. I can't speak to that specific file. I don't know if I

22   reviewed that specific file. Like I said, I did more

23   Confluence review and less of a Stash review, but.

24   Q. But you know the Stash documents that were released predate

25   April 16, right?

M6o5sch2   Leedom - Cross

1   A.   I don't remember the exact dates for the Stash, like, the

2   timing analysis for Stash, but I believe so.

3   Q.   Stash was much more valuable than Confluence, right?

4   MR. DENTON: Objection.

5   THE COURT: Sustained.

6   Q.   Stash contained the source code for all the CIA tools,

7   right?

8   A.   Contained the source code for tools developed on DevLAN.

9   Q.   Right. And Confluence was just a wiki, as you testified

10   about; right?

11   A.   Yes.

12   Q.   Stash contained much more sensitive data, correct?

13   A.   I don't know the classifications of either. I mean, they

14   were both sensitive things.

15   Q.   But the source code and the amount of source code here --

16   200 gigabytes -- is much more valuable than the small

17   Confluence data, right?

18   MR. DENTON: Objection.

19   THE COURT: Sustained. Lets move on, please.

20   Q.   There are also several other directories on the Altabackup

21   server, correct?

22   A.   Are you talking about the, like, the home folder and the

23   source in gold folder or the --

24   Q.   Yeah. There is many more directories or many more shares

25   on the Altabackup server, right?

M6o5sch2   Leedom - Cross

1   A.   I believe there is a handful of shares.

2   Q.   Just to be clear, the FS-01, that's the same thing as the

3   Altabackup server, right?

4   A.   Yes. So FS-01 is the server that has the home folders, all

5   the shares we are looking at now, as well as the separate share

6   for Altabackup. They are separate distinct things.

7   Q.   As part of your investigation did you review these shares?

8   A.   Yes, for what was available.

9   Q.   You reviewed the OSB test repo, correct?

10   A.   I think for the exact folders, I don't know what all from

11   this list of permissions there were actual folders for, but if

12   there was a folder on the server I reviewed it. I don't

13   remember at this point, it has been a long time. I can only

14   speak to the five folders I think at Exhibit 4 in the

15   presentation. Those, I remember. Outside of that, I don't

16   really remember.

17   Q.   And every DevLAN user could access this test repo or DS-00

18   directory, correct?

19   A.   I disagree.

20   Q.   You don't think this test repo can be reviewed by everyone?

21   A.   Well, everyone, you would have to have -- it needs to be on

22   Windows.

23   Q.   OK. Well, the permissions, I am talking access controls

24   only.

25   A.   Yes. As long as you are on the Windows part of the

M6o5sch2   Leedom - Cross

1 network, yes.

2 Q. Each of these directories held copies of Confluence too,

3 correct?

4 A. I don't know.

5 Q. You said you reviewed these directories, right?

6 A. I have never found copies of Confluence.

7 Q. And the OSB test repo or test 00 directory?

8 A. Like I said, I don't remember these other directories.

9 Q. OK. But from -- just from a forensic standpoint, you don't

10 know if WikiLeaks received every single backup off DevLAN,

11 correct?

12 A. I can't speak to what files they have, no.

13 Q. You don't know if WikiLeaks received every byte off DevLAN,

14 right?

15 A. Like I said, I can't speak to the actual files they have.

16 Q. Right. So all you can say is that WikiLeaks disclosed

17 information, right?

18 A. Yes.

19 Q. And that information was present in the backup starting

20 with March 3rd, 2016, right?

21 A. So I can definitively say that the content posted on March

22 7 for Confluence came from that March 3rd backup, that specific

23 backup.

24 Q. You found it came from the specific March 3rd backup?

25 A. From my analysis of it; yes, that's my opinion.

M6o5sch2   Leedom - Cross

1   Q. If WikiLeaks received a March 4th backup they would have

2   the same data, right?

3   A. From what I described I think it is highly likely they have

4   the March 3rd backup.

5   Q. That's not the question, though. The question is backups

6   after March 3rd, March 4th, March 5th, all those backups,

7   WikiLeaks could have those, right?

8   A. Like I said, I don't know exactly what they have.

9   Q. And all you know is that WikiLeaks disclosed information

10   starting up to March 3rd, right? The latest -- I'm sorry.

11   The latest data that WikiLeaks released is from March 3rd,

12   right?

13   A. From Confluence, from what I understand, yes.

14   Q. So to your knowledge, the information released by WikiLeaks

15   could have come from the offsite backup, right?

16   A. No.

17   Q. You said you didn't review the offsite backup?

18   A. No, I said I didn't --

19   THE COURT: I was just coughing but I think,

20   Mr. Schulte, we have covered this ground, so let's move it to a

21   new line, please.

22   Q. Based on the security logging and setup on DevLAN, the

23   official offsite backup, the foreign offices, the links, there

24   is absolutely no logging or mechanisms in place to trace who or

25   when the data was copied, correct?

M6o5sch2   Leedom - Cross

1   A. I can't speak to, like, all of those mechanisms. All I can

2   say is that like I asked for --

3   Q. Yes.

4   A.   -- network logs and never received any.

5   Q. Right.

6   So you didn't receive any of that because there is no

7   security logs -- let's touch base real quick on the NetFlow

8   logs.

9   MR. DENTON: Objection.

10   THE COURT: Let's let Mr. Schulte finish his question

11   but, Mr. Schulte, I think we are kind of going backwards here.

12   Let's go to new areas, please.

13   (Continued on next page)

14

15

16

17

18

19

20

21

22

23

24

25

M6oWsch3   Leedom - Cross

1 BY MR. SCHULTE:

2 Q. OK. Just very briefly, the NetFlow logs, those logs would

3 have shown data that was transferred along, across the network,

4 right?

5 A. That's something they could have shown.

6 Q. OK. Let's turn to slide 29 in your presentation. You

7 concluded that the data leaked by WikiLeaks must derive from

8 one of the backups generated by the backup script, correct?

9 A. Yes.

10 Q. Slide 31 is the key points to the backup script, correct?

11 A. Yeah, it's -- this is why there was a corrupted database.

12 Q. This is the mySQLdump command, right?

13 A. Yes.

14 Q. And as part of your investigation, you analyzed the

15 WikiLeaks data dump, right?

16 A. The release?

17 Q. Yes.

18 A. Yes.

19 Q. And you concluded that the WikiLeaks must suggest a

20 malformed database file, correct?

21 A. Correct.

22 Q. That's this .SQL file, correct?

23 A. That's correct.

24 Q. In order to obtain a pristine database, the mySQLdump

25 command had to be run in a special way, right?

```
 1    A.   Yes.

 2    Q.   But the command still required the passwords to the

 3    database, correct?

 4    A.   Yeah.  You had to authenticate to the database to be able

 5    to export it.

 6    Q.   And these passwords were found in the script, right?

 7    A.   They're patched in as variables.  They might be in the

 8    Python script that runs in the script.

 9    Q.   Yes.  And these -- so if someone accessed the server, they

10    could have simply run the backup script, correct?

11    A.   If someone had access to the server, yes, they could have

12    run the backup script.

13    Q.   They could have copied this mySQLdump command and run that

14    command, right?

15    A.   Like, directly on the command line?

16    Q.   Well, substituting variables and whatnot.

17    A.   Yes.

18    Q.   So in any case, your analysis does not conclude that the

19    data released by WikiLeaks derived from a backup on the

20    Altabackup, does it?

21    A.   Part of that also includes the, you know, access times for

22    those backup files.

23    Q.   No.  I'm just talking about this analysis, this analysis

24    you ran here.

25    A.   If you ran the mySQLdump command, it would create the same
```

1   kind of backup.

2   Q. OK. So in your presentation, you go through this entire

3   section. The leak came from the Atlassian backups, and this

4   entire section is based upon the script, right?

5   A. Yeah, the error that the -- that's introduced by this

6   command is really important.

7   Q. But you can only conclude that the files released by

8   WikiLeaks derived from a malformed SQL file, correct?

9   A. Say only conclude, but it definitely goes far to, like,

10   assisting with the conclusion, yes.

11   Q. But this, based on your analysis, this is not -- this

12   slide, 29, when you say the leak came from the Atlassian

13   backups, right, this is not a conclusion you can reach from

14   your analysis, is it?

15   A. I don't understand.

16   Q. If someone logged in to the Confluence machine and executed

17   the mySQLdump command with the same command line arguments from

18   the script, then the output SQL file would contain the same

19   error, correct?

20   MR. DENTON: Objection.

21   THE COURT: Overruled.

22   A. Yes, if you ran that mySQLdump command, the -- I mean

23   output file's going to be the same. It's the same command.

24   Q. And that output would not be an Altabackup file, right?

25   A. I don't understand. It's the same files that are on the

1   backup server. It's the --

2   Q. I mean your specific conclusion was that it came from the

3   Altabackup directory, right; that was your conclusion?

4   A. This specific portion of the presentation is just to

5   discuss the error with the database and why the WikiLeaks

6   publication looks like it does and that it came from one of

7   these corrupted backups, specifically the March 3 backup.

8   Q. We're just talking about this analysis. This does not have

9   anything to do with March 3 right now, right?

10   A. I mean this -- all of this, part 2 is all about the

11   analysis I did on that March 3 backup, so --

12   Q. But your analysis that you're running here is predicated on

13   backups from the official Altabackup store, correct?

14   A. Yes.

15   Q. OK. So the point is if somebody accessed the server and

16   ran this command, they could produce their own files, right?

17   A. Yeah, if you -- if you ran the mySQLdump command on March 3

18   at the same time as the one on the backup server, those

19   databases would be, like, almost identical.

20   Q. So just based on this analysis, it's possible that

21   WikiLeaks did not receive any backups from the Altabackups at

22   all, correct?

23   A. I disagree.

24   Q. OK. So from this analysis, you can determine that

25   WikiLeaks receives files specifically from the Altabackups

M6oWsch3   Leedom - Cross

1   directory?

2   A.   Sorry. Just having hard time -- like I said, the portion

3   of this, talking about the backup script, the error, it's not

4   so much about, like, whether it came from Altabackup. It's to

5   date it and show that what they had was from a corrupted backup

6   from that date. I don't really go to anything talking about,

7   like, a page on WikiLeaks that shows, you know, like, where it

8   came from.

9   Q.   OK.

10   A.   This specific stuff is just about that.

11   Q.   So the question is simply not -- it's not whether you agree

12   or disagree. The question is whether it's possible, based on

13   the forensic analysis of the script, that WikiLeaks received

14   files that were not from the Altabackups.

15   A.   I -- I can't speak to, like, exactly what they have, so --

16   I -- I'm just trying to say that if you ran the dump command,

17   it would be the same database that's on the backups.

18   Q.   OK.

19   A.   Whether it -- yeah, go ahead.

20   Q.   This is just the point. The point is you run this command,

21   you get a file, that file's not one of the official backups,

22   right?

23   A.   If you ran the command on the server, yes.

24   Q.   OK. And then that file got transmitted to WikiLeaks,

25   correct?

1   A.   I don't --

2   Q.   This is a possibility, right?

3   A.   We're talking about a theoretical scenario.

4   Q.   Yeah. I'm just saying is it possible. That's the

5   question.

6   A.   You could make a new backup if you had access, like, to the

7   server. Like, you could run these commands. As long as you

8   had permission to access the database, yes, you could run the

9   backup script.

10   Q.   OK. So based solely on your analysis on this backup

11   script, right, it's not forensically possible to determine

12   whether WikiLeaks received the file from the Altabackups or

13   not? Right?

14   MR. DENTON: Objection.

15   THE COURT: Sustained.

16   BY MR. SCHULTE:

17   Q.   OK. Based on your analysis on this, on the backup script,

18   right, your analysis of the corruption of the SQL file, that's

19   the conclusion that you made? Right?

20   A.   Yeah, and also reviewing the Confluence --

21   Q.   No. I'm just asking about this. I'm just asking about

22   your analysis on this specifically. We'll move on to the next

23   part later.

24   A.   Yeah. The post on WikiLeaks came from a corrupt database.

25   That's my testimony, and that's sort of -- that's what this is

1   meant to show.

2   Q. OK. And based on this, it's not forensically possible to

3   determine whether WikiLeaks received the file from Altabackup,

4   right?

5   MR. DENTON: Objection.

6   THE COURT: I'll allow it. Overruled.

7   A. So, the forensics, like, for this theory that we're talking

8   about now --

9   Q. It's just yes or no.

10   A. Can you rephrase the question? Or just restate would be

11   fine.

12   MR. SCHULTE: Can the court reporter reread it,

13   please.

14   THE COURT: The question is "based on this it's not

15   forensically possible to determine whether WikiLeaks received

16   the file from Altabackup, right"?

17   A. No. I disagree.

18   Q. You just said that somebody can run this command

19   separately, correct?

20   A. Yes, in this theoretical scenario, there would be

21   additional logs for this command being run, especially --

22   Q. We're just talking about the possibilities here.

23   MR. DENTON: Objection.

24   THE COURT: Sustained.

25   BY MR. SCHULTE:

1   Q. You testified that someone can run this script and produce

2   their own file, right?

3   MR. DENTON: Asked and answered, your Honor.

4   THE COURT: Sustained.

5   (Defendant conferred with standby counsel)

6   BY MR. SCHULTE:

7   Q. Sir, it's possible, correct, that WikiLeaks received a

8   different corrupt database?

9   A. I'd say no.

10   Q. Based on this analysis alone.

11   MR. DENTON: Objection.

12   THE COURT: Sustained.

13   BY MR. SCHULTE:

14   Q. This analysis you did on the backup script, right --

15   A. So --

16   Q. I'm just talking about this analysis. We'll talk about the

17   other thing later.

18   A. I don't think talking about this is enough to qualify that

19   statement. There's a lot of other things you need to take into

20   account.

21   Q. Like what?

22   A. On the Confluence server, especially on March -- March 3,

23   there's -- there would be logs and history, command history or

24   even, like, in unallocated space, for, like, this type of

25   command being run, and we know this command would have had to

1 have been run on March 3 to make the same backup, so there's --

2 there's no evidence of that.

3 Q. Well, you don't know that the March 3 backup was stolen,

4 correct?

5 A. I don't understand. It --

6 Q. You've testified that the backups after March 3 contained

7 the same data, right?

8 A. It could.

9 Q. OK. So you can't say that it had to be -- the command had

10 to be run on March 3, right?

11 A. I think I go a long way to showing that with this part of

12 the presentation. I --

13 Q. If someone on, you know, in December accessed the server

14 and ran this command, it would contain the same data WikiLeaks

15 had, right?

16 A. It could potentially have the data from before.

17 Q. OK.

18 A. It's -- I don't think you'd be able to, you know, make an

19 accurate one-to-one, like, March 3 copy without actually having

20 the March 3 copy to, like, compare from. Just from what was

21 missing in that database, I just don't think there's enough

22 information there.

23 Q. I thought your testimony on direct was that it was

24 possible; it would just take work.

25 A. Yeah, it would be a significant amount of work. I think --

1   Q.   That's all I'm asking. It's possible, right?

2   MR. DENTON: Objection, your Honor. Can the witness

3   finish the answer?

4   THE COURT: Sustained.

5   Go ahead, Mr. Leedom.

6   A.   Yeah, and something that would be a big part of that would

7   be, like, having to have that older backup. I think from,

8   like, looking at what we reviewed and that it was clear they

9   tried to get every morsel out of what was in there. So, in my

10 opinion, if they had a later backup, we would see every morsel

11 of what was in there from a later date, not from March 3.

12 Q.   That's just your speculation, though, right?

13 A.   My opinion.

14 Q.   Because, like you said, you don't know actually what files

15 WikiLeaks had, right?

16 A.   I don't know exactly what files were on their server, no.

17 Q.   And you testified they tried to get every morsel of data

18 out of March 3, right?

19 A.   My opinion.

20 Q.   Right. So if they had a later backup and they restricted

21 themselves to March 3, it would be the same, right?

22 A.   Well, if you're restricting yourself, you're not getting

23 every morsel out of it.

24 Q.   Well, you'd get every morsel out of the March 3 data,

25 right?

M6oWsch3   Leedom - Cross

6   Q. Just to be clear here, opening a file automatically updates

7   the access time, correct?

8   A. You said opening a file?

9   Q. I'm sorry. You didn't hear?

10   A. Did you say opening a file?

11   Q. Opening a file updates the access time, right?

12   A. Yes.

13   Q. OK. Access time only tells you one thing, correct?

14   A. Could be multiple things but this tells you last time the

15   file was opened for reading, yes.

16   Q. The access time only tells you the file was accessed,

17   right?

18   A. That's correct.

19   Q. Does not forensically indicate that the file in question

20   was copied, correct?

21   A. Other than that you can read what's in it, no.

22   MR. SCHULTE: So let's take a look at -- one second.

23   Q. So you're -- there's no forensic artifact to support the

24   notion that those specific files from Altabackup were ever

25   provided to WikiLeaks, correct?

M6oWsch3   Leedom - Cross

1   A.   Other than the step we've talked about previously, there's

2   no forensic artifact of, like, a copy command for those files,

3   no.

4   Q.   Do you know about the Linux touch command?

5   A.   Yes.

6   Q.   This command can be used to change file times, right?

7   A.   Yes, it can.

8   Q.   That includes access times, right?

9   A.   Yes.

10   Q.   And from reviewing my workstation, you know that I

11   developed Linux malware tools for the CIA, right?

12   A.   I know you worked on a few tools. I don't know if they

13   were Linux-specific or not, but --

14   Q.   And you knew from that that I wrote malware that

15   specifically used the touch command to change file times,

16   right?

17   MR. DENTON: Objection.

18   THE COURT: Overruled.

19   A.   I don't know about the specifics of the code you wrote.

20   Q.   You did not review any of the source code?

21   A.   I reviewed -- it was a long time ago, and like I said, I

22   didn't review, like, every single project either.

23   Q.   OK. But would you not agree that malware developers know

24   how to change file times?

25   A.   I can say sometimes malware time stomps files.

1   Q.   OK.

2   THE WITNESS: Time stomp, that's what we call it.

3   I can explain.

4   THE COURT: Go ahead.

5   THE WITNESS: So, when, like, a malicious actor or

6   malware, usually when they're, it's, like, when they're

7   cleaning up, they will change file time stamps for files to

8   make it look like, you know, if they edited a file; they'll

9   make it look like it was edited on an earlier date. In the

10   field, that's called time stomping.

11   BY MR. SCHULTE:

12   Q.   And it would take only a few seconds to type a touch

13   command to replace the access times, right?

14   A.   It's a short command.

15   Q.   And in fact, Windows also has a very simple command to

16   change file times, correct?

17   A.   I think it's a bit more complicated in Windows.

18   MR. SCHULTE: All right. I'm going to show the, just

19   the parties and the witness what's marked as defense exhibit

20   1206-1.

21   Q.   And do you know what this is?

22   A.   Looks like a API, Windows API call.

23   Q.   And what does Windows API mean?

24   A.   Programmatically, if you want to perform an action on

25   Windows, there's a set of, kind of predefined, we'll call

1   functions that you use that will do that for you. So this is

2   one of those.

3   Q. So when writing source code, you use Windows API to do

4   that, right?

5   A. Yes. This would be something you have to, like, actually

6   write out a program to do.

7   Q. And Windows documents all their calls so that developers

8   can use them, right?

9   A. Not all of them, but there are most that are documented.

10   MR. SCHULTE: I move to introduce 1206-1.

11   MR. DENTON: Objection.

12   THE COURT: Sustained.

13   (Defendant conferred with standby counsel)

14 BY MR. SCHULTE:

15 Q. Well, you recognize what this API is, right?

16 A. I mean I can -- I haven't used it. I can read the

17 description, what it's for.

18 Q. And this is a technical document, correct?

19 A. Yes.

20 Q. It describes how technical code can be used, right?

21 A. Yes.

22   MR. SCHULTE: Now can I move this into evidence?

23   MR. DENTON: Same objection.

24   THE COURT: Same ruling.

25   Let's keep going, Mr. Schulte.

M6oWsch3   Leedom - Cross

1   BY MR. SCHULTE:

2   Q. OK. Are you aware of a function in Windows to change file

3   times?

4   A. Yes, I know it's possible.

5   THE COURT: Let's take this down, please.

6   MR. SCHULTE: I'm just going to show the witness

7   what's marked as 1206-2.

8   Q. And Windows, just like in Linux, it's -- there's a function

9   call to change the times, right?

10   A. So, in Linux, you're talking about a command that you would

11   run, like a touch command that you'd run. This is, like,

12   something you'd have to write a program for. It's different.

13   Q. OK. But it's one command, relatively short to do it,

14   right?

15   A. I think writing a program to achieve this is a lot more

16   effort than typing, like, the touch command, for example,

17   but --

18   Q. OK. But it would be a very small program or very -- it

19   wouldn't take very many lines of code to do it?

20   MR. DENTON: Objection.

21   THE COURT: Sustained.

22   Let's move on, Mr. Schulte.

23   BY MR. SCHULTE:

24   Q. If an intruder noticed the April 20, 2016, access time on

25   the March 3, 2016, backup, they easily could have chosen to

M6oWsch3   Leedom - Cross

1   release files from March 3, 2016, to WikiLeaks to plant a false

2   flag, correct?

3   A.   I can't speak to the, like, the -- I don't know, like, what

4   an intruder's thought process would be.

5   Q.   It's just if it's possible.

6   MR. DENTON: Objection.

7   THE COURT: Sustained.

8   BY MR. SCHULTE:

9   Q.   Do you know what a false flag is?

10   MR. DENTON: Objection.

11   THE COURT: Sustained.

12   (Defendant conferred with standby counsel)

13 BY MR. SCHULTE:

14 Q.   As part of your experience, training, investigation, do you

15 know or have you researched the false flags?

16   MR. DENTON: Objection.

17   THE COURT: Sustained.

18   (Defendant conferred with standby counsel)

19 BY MR. SCHULTE:

20 Q.   During this investigation, did you look for false flags?

21 A.   To the extent that you can, like, look for false flags, I

22 mean it's -- any kind of unauthorized, like, access to the

23 network would be something we looked for.

24 Q.   I'm sorry. So your testimony is you looked for them as

25 much as you could?

M6oWsch3   Leedom - Cross

1   A.   From what we, from what evidence we gathered, it was, you

2   know, it's part of something you -- you analyze evidence with.

3   If you see, like, if there, like -- there wasn't any, but if

4   there was, like, an event where someone had accessed the

5   network, then, yeah, you would review, like, where that came

6   from and, like, try to make some sense of the reasons behind

7   it. Like, to the extent you're looking for a false flag,

8   that's what you would do, but from our review, we never found

9   anything that would indicate that.

10 Q.   But false flags generally are difficult to discern,

11 correct?

12 A.   Not always.

13 Q.   Have you heard of the Olympic Destroyer malware that

14 disrupted the Olympic Games in 2018?

15   MR. DENTON: Objection. Relevance.

16   THE COURT: Sustained.

17 BY MR. SCHULTE:

18 Q.   Through your position and expertise, you research and learn

19 about operations that are occurring in the wild, correct?

20 A.   I do.

21 Q.   OK. So based on your expertise and experience, did you

22 know about the Olympic Destroyer malware from 2018?

23   MR. DENTON: Objection.

24   THE COURT: Sustained.

25   (Defendant conferred with standby counsel)

M6oWsch3   Leedom - Cross

1   BY MR. SCHULTE:

2   Q. Did you know that malware used false flags to mislead

3   reverse engineers?

4   A. Yes.

5   Q. And you're a reverse engineer, correct?

6   A. I've done reverse engineering in the past.

7   Q. And from your review on this case, did you know it was

8   common practice at the CIA to plant false flags?

9   MR. DENTON: Objection.

10   THE COURT: Sustained.

11   BY MR. SCHULTE:

12   Q. Did you know every developer on DevLAN had training in

13   miss --

14   MR. DENTON: Objection.

15   THE COURT: Sustained.

16   Let's move on, Mr. Schulte.

17   BY MR. SCHULTE:

18   Q. You testified on direct about the snapshot from April 16,

19   2016, right?

20   A. Yes.

21   Q. And I think that's slide 68 in your presentation.

22   MR. SCHULTE: Pull that up.

23   Q. This snapshot was named BKUP 4-16-2016, right?

24   A. Yes.

25   Q. And BKUP is a common nomenclature for backup, right?

1   A.   I don't know how common it is. I think it's clear it

2   stands for backup.

3   Q.   OK. Did you check whether the Confluence backup access

4   time was a direct byproduct of the Confluence snapshot itself?

5   A.   It was not.

6   Q.   Did you investigate that?

7   A.   Yes.

8   Q.   Did you replicate the DevLAN network?

9   A.   You can't replicate the DevLAN network.

10   Q.   You couldn't replicate the DevLAN network?

11   A.   No.

12   Q.   Why?

13   A.   I mean by the time we got there, it was a year after this

14   time frame, and there had been a lot of changes to that

15   network.

16   Q.   You were aware that Dave C. and Jeremy Weber took the April

17   16, 2016, snapshot, correct?

18   A.   Yeah, that, that weekend. I think it was -- I don't know

19   which one of them did it, but --

20   Q.   If they initiated a process or cron job that ultimately

21   touched the March 3, 2016, backup file, it would have been

22   preserved in the snapshot, right?

23   A.   Before or after they took the snapshot?

24   Q.   Well, before, during.

25   A.   If they ran a cron job to -- if they ran a cron job before

M6oWsch3   Leedom - Cross

1   taking the snapshot -- well, yeah, they didn't do any

2   reversion, so, yes. I don't remember seeing anything like that

3   from my review.

4   Q. The question was just would that be preserved in the

5   snapshot?

6   A. If it happened before the snapshot was taken, yes.

7   Q. So in this case, on April 16, 2016, the March 3, 2016,

8   backup would have been accessed, correct?

9   A. No.

10 Q. It wouldn't have been?

11 A. I don't understand. This is just a snapshot that's being

12 created. This has nothing to do with the backups or anything.

13 Q. Well, the question is if they initiate a process or cron

14 job that ultimately touched the file, then it would have been

15 accessed on that day, right?

16 A. I can't speak to, like, the theoretical if they did

17 something. I -- reviewing the machine I did not see anything

18 like that.

19 Q. Just forensically, is this possible?

20 A. At any point if you access the file, the access time would

21 change.

22 Q. OK. So if this was preserved in the snapshot on April 16,

23 it would have updated the access times, right?

24   MR. DENTON: Objection to form.

25   THE COURT: Sustained.

1   BY MR. SCHULTE:

2   Q. Is it possible forensically that the process or cron job

3   was initiated prior to the snapshot on April 16, 2016?

4   MR. DENTON: Objection to form.

5   THE COURT: Sustained.

6   I'm not sure I understand the question, Mr. Schulte.

7   MR. SCHULTE: OK. So let me just go back and ask this

8   question.

9   Q. Jeremy Weber and Dave C., if they initiated a process or

10   cron job that ultimately touched the March 3, 2016, backup

11   file, it would have been preserved in the snapshot, right?

12   THE COURT: That we've already covered, so a new

13   question.

14   MR. SCHULTE: OK.

15   Q. So in that case, then on April 16, 2016, the March 3, 2016,

16   backup would have been accessed, right?

17   A. If they did that and it was accessed on the 16th, then the

18   access time would be for April 16.

19   Q. Yes.

20   A. But the access time's not April 16. It's April 20.

21   Q. I understand that, but -- OK.

22   And if that were the case, the next question was you'd

23   expect the March 3, 2016, backup to show an April 16, 2016,

24   access time, right?

25   A. If they accessed it on the 16th, then yes.

M6oWsch3   Leedom - Cross

1   Q. OK. So when the Confluence was reverted back to the April

2   16 snapshot, it would have executed the same cron job and

3   touched the March 3, 2016, Confluence backup file again,

4   correct?

5   MR. DENTON: Objection. Compound, hypothetical, your

6   Honor.

7   THE COURT: Sustained.

8   BY MR. SCHULTE:

9   Q. So when Confluence was reverted back to the April 16, 2016,

10 snapshot, it would have executed the same cron job, right?

11   MR. DENTON: Same objection.

12   THE COURT: Sustained.

13   (Defendant conferred with standby counsel)

14 BY MR. SCHULTE:

15 Q. OK. Let's talk a little bit about the permission change in

16 the April 16, 2016, snapshot. All right? On the next slide,

17 69, shows a list of authorized SSH keys before the snapshot,

18 right?

19 A. That's correct.

20 Q. And 70 shows that all the SSH keys were removed, right?

21 A. Yes.

22 Q. And then a new one was added, right?

23 A. Yes.

24 Q. And the only way you concluded that the April 16, 2016,

25 snapshot maintained my previous privileges is by actually

1   reverting to the snapshot, right?

2   A.   Yes.   We have the snapshot.

3   Q.   But you would agree that there would be absolutely no way

4   for anyone to know the state of the virtual machine in the

5   April 16, 2016, snapshot, right?

6   A.   There -- I mean I think I -- I can't speak to what everyone

7   knew on the network, but wasn't there an email that was -- that

8   said, like, the changes happened that weekend?

9   Q.   No, no.   The question is there's no way to see what

10   permissions exist in the snapshot, right?

11   A.   Without -- you'd have to go into the snapshot and, like,

12   view the system at that time.

13   Q.   You'd have to actually execute the snapshot -- you'd have

14   to revert to the snapshot, right?

15   A.   If you wanted to look at files from that snapshot, yes.

16   Q.   If you wanted to see what accesses were in that snapshot,

17   right?

18   A.   There would be the file in the snapshot.

19   Q.   OK.   So this, your slides here, 69, 69 and 70, you don't

20   know this information from the snapshot, right?

21   A.   Like, looking at the -- I'm confused.   The data in the

22   snapshot?

23   Q.   No, no.

24   A.   Or --

25   Q.   Yeah.   I'm sorry.   So outside.   Without looking, without

1   running the reversion, you don't know any of this, right?

2   A.   The only thing you know about the snapshot without

3   reverting the snapshot is what's in the, like, I don't know if

4   it's the previous slide, where it shows the snapshot

5   information, just, like, a time stamp and name, things like

6   that.   That's all you'd know about the time stamp -- or the

7   snapshot.

8   Q.   OK.   And then once you revert it, then that's when you

9   could learn the privileges changes, right?

10   A.   Yes.

11   Q.   Have you ever been a system administrator before?

12   A.   I have in some capacities.

13   Q.   Have you ever managed Enterprise system with multiple

14   virtual machines?

15   A.   Yes.

16   Q.   So you know the process of taking a snapshot is a common

17   system administration, correct?

18   A.   Yes.   I think I've said that too in previous testimony.

19   Q.   OK.   Taking a snapshot's not an inherently harmful computer

20   command, correct?

21   A.   No.

22   Q.   The process of reverting a snapshot is also a common system

23   administration, correct?

24   A.   In some circumstances, yes.

25   Q.   Just whether this is common in system administration.

1   A.   It's something that you would do for certain reasons.

2   Q.   And reverting a snapshot is not an inherently harmful

3   computer command, correct?

4   A.   It's harmful to the state of that machine. If you revert

5   to a -- if you have a snapshot from one month ago and I revert,

6   then I'm going to lose everything that happened for the last

7   month, so it is a -- I don't want to use the word

8   "destructive," but it is a -- it will, you know, delete that

9   information.

10   Q.   But it's still, it's still common to run this in system

11   administration practices, correct?

12   A.   Like I said, for some instances, yes, you would revert a

13   virtual machine.

14   Q.   If you're going to, if you need to roll back a system,

15   right?

16   A.   Yes.

17   Q.   And deleting a snapshot is not an inherently harmful

18   computer command, correct?

19   A.   No.

20   THE COURT: All right. We're going to take our break

21   now.

22   Ladies and gentlemen, a couple standard reminders.

23   Don't discuss the case. Keep an open mind. Don't do

24   any research about the case.

25   It's 11:40. Let's get going promptly at 12:20, so

1   please be ready to go beginning at 12:15.

2   With that, I'm going to excuse you. Enjoy your break.

3   Thank you.

4   (Continued on next page)

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1   (Jury not present)

2   THE COURT: You may be seated.

3   Mr. Leedom, I remind you that you shouldn't discuss

4   the substance of your testimony with anyone from the government

5   during your break since you remain on cross. Please be here or

6   be in the witness room by 12:15 and ready to go.

7   THE WITNESS: Yes, sir.

8   THE COURT: With that, you may step down.

9   Mr. Schulte, any estimates of how much longer you

10 have? I have to say the pace of this I'm finding quite

11 difficult.

12   MR. SCHULTE: Yes. I'm trying to touch on everything.

13   THE COURT: I'm just asking for a time estimate.

14   (Witness not present)

15   MR. SCHULTE: Yeah. I mean from this, I have, maybe,

16 half of what we've gone through already. So from, we start

17 9:30 to 12, half of that, an hour and a half or two hours,

18 maybe.

19   THE COURT: OK. I would really urge to try to pare

20 things back. First of all, I think a lot of the technical

21 details are completely lost on the jury. I think there's a lot

22 of repetition, a lot of questions that are being asked and

23 answered multiple times, and I'm just going to start forcing

24 you to move along. It's just not a tolerable pace and I don't

25 think you're making a whole lot of productive use of the time

1   you're being given other than establishing that there's no

2   forensic evidence of codes copied with external drives or

3   anything of that sort. It's just not clear to me what you've

4   accomplished in most of this cross, so I'm going to start to

5   force you to use your time a little bit more wisely and

6   valuably.

7   Anything to discuss before I give you your breaks?

8   Mr. Denton.

9   MR. DENTON: Not from the government, your Honor.

10   THE COURT: Mr. Schulte.

11   MR. SCHULTE: No.

12   THE COURT: All right. Please be back by 12:15, and

13 we'll get going promptly. Thank you.

14   (Luncheon recess)

15

16

17

18

19

20

21

22

23

24

25

M6o5sch4   Leedom - Cross

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

2   12:15 p.m.

3   (Trial resumed; jury present)

4   THE DEPUTY CLERK: Jury entering.

5   THE COURT: Welcome back, ladies and gentlemen. I

6   hope you enjoyed your break. We will continue with the

7   cross-examination of Mr. Leedom.

8   You remain under oath, Mr. Leedom.

9   THE WITNESS: Yes, sir.

10   THE COURT: Reminder, again, to please move the

11   microphone closer, speak slowly, clearly and into the

12   microphone. And, you may remove your mask.

13   You may proceed, Mr. Schulte.

14   BY MR. SCHULTE:

15   Q. Before we went to lunch we were talking about snapshots and

16   reversions and system administration. As part of your

17   investigation you stated that you reviewed my CIA workstation,

18   correct?

19   A. Yes.

20   Q. And through your investigation -- I'm sorry. Let me

21   restate.

22   And your investigation revealed that I regularly took

23   snapshots and reversions, correct?

24   MR. DENTON: Objection.

25   THE COURT: Sustained.

M6o5sch4   Leedom - Cross

1   Q.   In your investigation of all developers' systems did you

2   determine that snapshots and reversions were common and regular

3   practice on DevLAN?

4   A.   I don't recall, really, the exact frequency. I mean, there

5   were developers that used virtual machines and I assume had

6   snapshots but I can't speak to their, like, normal everyday

7   practice, really.

8   Q.   Let's discuss the reversion for a minute. A reversion is

9   when you go back to a point in time, correct?

10   A.   Yes, a point when you go to a previous snapshot.

11   Q.   And during the time you are in a reversion, the system

12   itself is still running, correct?

13   A.   No.

14   Q.   When you are in a reversion the system is not running?

15   A.   Are you talking about, like, the process while it is

16   reverting? Or --

17   Q.   No, once you have done the reversion. Once you executed

18   the reversion the system is still running, right?

19   A.   If the snapshot was taken while the system was running it

20   would be just as it was when the snapshot was taken.

21   Q.   And others who may be unaware of the reversion are still

22   working on their projects, right?

23   A.   I don't understand.

24   Q.   So other people who are working on Confluence, they would

25   not know that there has been a reversion, right?

M6o5sch4   Leedom - Cross

1 A. From what I understand, the way that system worked there

2 wasn't any of the -- there are -- let me explain this. So

3 there are features of certain versions of ESXi that support --

4 I don't know what the term is but a type of reversion where if

5 a user was using the system they wouldn't notice but in this

6 case, like, if you were currently trying to edit a page and

7 then it got reverted, you would have to log back in again.

8 Q. So if changes are being made this would be noticeable,

9 right?

10 A. Can you explain?

11 Q. It is fair to say that anyone who worked on Confluence

12 documents during the reversion period would lose their work

13 that they added when the system reverted back to the present

14 state, right?

15 A. I believe so. Yeah.

16 Q. It is fair to say that a person would realize that data

17 would have been lost by the reversion, correct?

18 A. Yes.

19 Q. Confluence documents were on the DevLAN system, correct?

20 A. The Confluence server was on DevLAN.

21 Q. And DevLAN was accessible from at least two different

22 vaults, correct?

23 A. I don't know exactly how many or which vaults, but yes.

24 Q. There is one on the eighth floor, right?

25 A. I don't remember which floor.

M6o5sch4   Leedom - Cross

1   Q. But you don't, through your investigation, you didn't learn

2   what floors DevLAN was on?

3   A. I did during the investigation but today I just don't

4   remember.

5   Q. But you know there were at least two different floors that

6   this was on, right?

7   A. I believe there were multiple floors that the group

8   operated on.

9   Q. And you testified on direct that there were about 200

10   employees in all this DevLAN space put together, correct?

11   A. Yes, about 200.

12   Q. And you were at the CIA during your investigation, correct?

13   A. Yes.

14   Q. For months at a time, right?

15   A. Yes.

16   Q. And you observed how the CIA employees worked, correct?

17   A. Which employees?

18   Q. The developers.

19   A. No.

20   Q. You didn't work with any of the developers at all?

21   A. I wouldn't say any but, like, we were very much -- what's

22   the word -- like isolated from all of the people and developers

23   for DevLAN. I think there might have been one or two

24   developers that we spoke to for, like, for some questions, but

25   not like any kind of regular contact.

M6o5sch4   Leedom - Cross

1   Q. OK. But through your investigation into the forensics, you

2   learned that developers typically worked well past 5:30,

3   correct?

4   A. People had different schedules. Some people worked later.

5   Q. I mean, you know that working for the CIA isn't a 9:00 to

6   5:00 job, right?

7   A. Correct.

8   Q. And that at 5:30 p.m. on April 20th, there were at least 15

9   developers still working in the vaults, right?

10 A. I don't remember.

11 Q. You don't remember how many people were actually in the

12 vaults on April 20th?

13 A. Not at this time. The only thing I remember from that

14 metric is the vault that you closed. I don't remember the

15 details from the other vaults at this time.

16 Q. Well, performing a snapshot and reversion at 5:30 would

17 have been very noticeable, right?

18 A. It depends.

19 Q. You just testified that people would know that their

20 products aren't being -- the work would be lost, right?

21 A. Only if you were, like, editing or updating a page on

22 Confluence.

23 Q. So if you were working during this time this would be

24 noticeable, right?

25 A. It really depends on what you are doing. If you are just

M6o5sch4   Leedom - Cross

1   viewing a page an hour is not a super long period of time, even

2   in a work day.

3   Q. You said you would have to log in again, correct?

4   A. Yes. It would probably ask you to, re-prompt you for login

5   which depending the last time you have logged in may not be

6   very noticeable or expected.

7   Q. It certainly would have been noticed unless there was a

8   heads up sent out about it, correct?

9   MR. DENTON: Objection.

10   THE COURT: Sustained.

11 Q. Typically, in system administration you would send out a

12 notice before doing something like this, right?

13 A. Yeah, making some kind of a, like a change like that,

14 that's going to happen while users are using the system, that

15 would be something that I think would be normal practice.

16 Q. Because this is the Confluence system, it is a production

17 system, right?

18 A. It is.

19 Q. And in the course of your investigation you learned that

20 there was a chat feature in Confluence, correct?

21 A. I think there was, like, a comment feature.

22 Q. No, I'm talking like instant messaging feature.

23 A. I don't remember an instant messaging feature in

24 Confluence.

25 Q. You don't recall individual users sending messages on the

M6o5sch4   Leedom - Cross

1   system?

2   A.   I know there was an IRC chat on the network.

3   Q.   But you don't recall any chat feature that was actually in

4   the web browser for Confluence?

5   A.   Not that I remember at this time.

6   Q.   That would have been part of your investigation, right?

7   A.   Yes. If there was content from that that was relevant I

8   would have reviewed it.

9   Q.   So through your investigation you don't recall any

10   message -- global message going out about the Confluence

11   system?

12   A.   There was an e-mail that was sent about the migration that

13   was going to happen on the 25th, but.

14   Q.   No, I'm talking on DevLAN; through your investigation, did

15   you not learn that there was a global message sent about the

16   Confluence downtime on April 20th?

17   A.   No, I don't -- I don't remember.

18   THE COURT: You don't remember at all or you don't

19   remember there being such a message?

20   THE WITNESS: I don't remember there being such a

21   message.

22   BY MR. SCHULTE:

23   Q.   You testified that deleting the April 20th, 2016 bkup

24   snapshot on the system, right?

25   A.   Yes.

M6o5sch4   Leedom - Cross

1   Q.   OK.

2   A.   Or -- excuse me. No, not the 4/16 snapshot.

3   Q.   The snapshot, the name was bkup?

4   A.   Just bkup.

5   Q.   Yeah, so you testified that deleting this snapshot, bkup,

6   deleted data on the Confluence system?

7   A.   The process of reverting and deleting it, yes.

8   Q.   I'm just talking about just deleting the snapshot?

9   A.   If you just delete the snapshot in a vacuum while you are

10   running past it, as long as you are past it then it deletes the

11   mile marker but no content from that is deleted as long as the

12   system is still running. It is the reversion portion that

13   really creates the deletion.

14   Q.   So I'm just saying the deletion of the April 20th snapshot

15   did not delete any data from the system, right?

16   A.   No. No, just deleting the snapshot itself after you have

17   reverted to it, that doesn't remove anything. It is the

18   reversion portion that does the deletion.

19   Q.   And the deletion is not -- it is just inherent to the

20   reversion process, right?

21   A.   No. You have to specifically delete it. When you revert

22   it doesn't, you know, it doesn't even automatically say, like,

23   delete, it is just you revert it and then you have to manually

24   go in and delete it afterwards.

25   Q.   I'm sorry, no. I'm talking about when you do, when you

M6o5sch4   Leedom - Cross

1   revert -- when you actually execute a reversion to another

2   snapshot, right, the loss of data is inherent in the reversion

3   itself, right?

4   A.   Yes.

5   Q.   So you are not actually going through and deleting files or

6   anything like this, right?

7   A.   By the process of reverting you have deleted everything,

8   not just files, but everything that's happened in the last

9   however long it was.

10   THE COURT: In other words, just to translate, when

11 you revert to an earlier backup you would lose any changes that

12 were made between the time that that snapshot was initially

13 made and the reversion to snapshot; is that correct?

14   THE WITNESS: That's correct.   It also works the other

15 direction as well.

16   THE COURT: What do you mean by that?

17   THE WITNESS: So in this case we had created a backup

18 at the current time and reverted to an old one and then did

19 some stuff and then reverted back to the current one.   So that

20 period of time that is sandwiched in between there is what gets

21 erased.

22 BY MR. SCHULTE:

23 Q.   I want to move on and show your slide presentation on slide

24 82.   Shell history or bash history typically records input like

25 this, right?

M6o5sch4   Leedom - Cross

1   A. The commands that are run, yes. The shell.log and ESXi is

2   a little more verbose.

3   Q. But the point is you are recording -- these files record

4   user's input to the system, correct?

5   A. Yes; commands that were executed.

6   Q. ESXi, like you said, specifically writes the commands to a

7   shell.log file, right?

8   A. Yes.

9   Q. But by default it does not record the output of the

10 commands, correct?

11 A. That's correct. I don't even think you can configure it to

12 do that.

13 Q. That's right.

14   Let's turn to slide 116. So this is not normal system

15 logging, correct?

16 A. Correct.

17 Q. This shows command input and output, correct?

18 A. That's correct.

19 Q. And these are known as transcript files, correct?

20 A. That is one method that this data could be logged, yes.

21 Q. And you testified at length about these transcript files

22 from my CIA work station, correct?

23 A. Yes, about these, yeah, the logs that we have shown here.

24 Q. Let me take it down and just show the witness what has been

25 marked as Defendant's Exhibit 1207. This is an online manual

M6o5sch4   Leedom - Cross

1 page, right?

2 A. It appears to be.

3 Q. And you know that Linux has a script command, correct?

4 A. I don't think I have ever used it, but reading the page it

5 seems like --

6   THE COURT: This isn't it evidence so don't read what

7 is on this page. Just answer based on your knowledge, please.

8 A. I haven't used this specific command but seems likely, yes.

9 Q. But the script command creates transcript files, correct?

10 A. Like I said, I haven't used it. I can look at the

11 documentation and explain from that but I haven't personally

12 used it. I'm not sure that I am allowed to say here.

13   MR. SCHULTE: I move to introduce this Exhibit 1207.

14   MR. DENTON: Objection.

15   THE COURT: Sustained.

16 Q. You testified that you are familiar with system

17 administration, right?

18 A. Yes.

19 Q. And that you have managed large servers before, correct?

20 A. I have managed servers before.

21 Q. And it's common practice for a system administrator to

22 record their actions to keep a record for other system

23 administrators, correct?

24 A. It depends.

25 Q. I mean, you want to record if something goes wrong, right?

M6o5sch4   Leedom - Cross

1   A.   It really depends on what your individual policies are on

2   the network and who you are working with and what types of

3   systems you are working on.

4   Q.   OK.   But it's good practice to essentially record actions

5   taken on enterprise systems, correct?

6   A.   Yes.

7   Q.   And system administrators do this through the script

8   command, correct?

9   A.   Like I said, I haven't used it but if a script command, you

10   know, could create a log of that then, yes, I suppose you could

11   use it for that but I haven't personally used it.

12   Q.   I am going to bring back up the 1703.   This script command

13   is the one that generates transcript files like these, correct?

14   MR. DENTON: Objection.

15   THE COURT: Sustained.

16   Q.   Is one way to generate files like this to use the script

17   command?

18   MR. DENTON: Objection.

19   THE COURT: I will allow it.

20   A.   I'm not familiar, like I said, with the exact output of the

21   script command, but.

22   Q.   So to your knowledge, how were these files created?

23   A.   So I know you can have, like, command logging enabled for

24   the terminal session itself and there is various ways that

25   things like this displayed on the screen can eventually end up

1   on disk. Like I said before, since we were looking at this,

2   like, the year afterwards, I wasn't surprised to see something

3   like this and, like, for the script command, I don't

4   remember -- I don't recall ever seeing script command run in

5   this time frame looking at command history on the machine

6   either. So there is various different ways this information

7   could show up.

8   Q. But you don't recall there being any other transcripts on

9   my CIA workstation except from April 20th, correct?

10   A. I mean, there are similar artifacts to this from -- I

11   believe, like, from the 18th.

12   Q. But I mean there is no, from April 20th until I resigned in

13   November, there is no other files like this on the system,

14   correct?

15   A. So this isn't, like, a file, really, this is a portion of

16   space that was on the virtual machine that is marked as

17   unallocated, it doesn't have any relationship to, like, an

18   individual file or files for that matter. This is essentially

19   just data that's remaining on the disk, so.

20   Q. Yeah. The question was did you see any file or any data

21   like this on the workstation from April 20th until I resigned

22   in November?

23   A. I don't know the absolute last timestamp entry or anything

24   from that machine. This activity was presented for being in

25   the April 20 time frame. I don't know or remember what was

M6o5sch4   Leedom - Cross

1   there from after that.

2   Q. But the only reason you have these files to exhibit here is

3   because the script command or other user intervention was used

4   to record this data, correct?

5   A. No. I can't say that at all.

6   Q. Then how was this file created?

7   A. I can't say that it was from user intervention. I mean,

8   just the way computers operate what can end up in memory from

9   using a terminal session or if it is saved to a file, things

10   get saved to disk. I really can't say.

11   Q. But normally -- you agree, normally, you don't see output

12   like this, correct?

13   A. Correct.

14   Q. And the terminal itself does not log that, correct?

15   A. You can configure it, too.

16   Q. That would require user intervention, correct?

17   A. Yes, you can say that.

18   Q. You testified on direct that when somebody does something

19   nefarious or deletes documents that that's what you called a

20   clue for your investigation; correct?

21   A. Yes.

22   Q. So wouldn't the fact that an individual purposefully

23   recorded a session also be important to that analysis?

24   A. It would be but, like I said, I don't have any evidence of

25   that.

1   Q. OK. So your testimony is that you simply don't have any

2   idea about how or why these files were created?

3   A. No.

4   Q. All right. Let's move on to slide 62. So my key was never

5   removed from the ESXi server, correct?

6   A. That's correct.

7   Q. And it was on the ESXi server from the time I set it up in

8   2014 until the time I left the agency in November 2016, right?

9   A. I don't know the exact first date that it was -- it would

10   have been on there but I know it was there when it was seized

11   so it was still there.

12   Q. It was still there a year after I left?

13   A. I believe so.

14   Q. And this key is sitting on the ESXi server in plain sight,

15   right?

16   A. The public key? Yes, it is an authorized keys file.

17   Q. There is no attempts to hide it, correct?

18   A. It's a normal file that's used for operation, so.

19   Q. And accessing a server using a key is very common, right?

20   A. Yes.

21   Q. Basically the same as someone using keys to unlock and open

22   their front door, right?

23   A. That's correct.

24   Q. And from your forensic examination you confirm that I

25   always logged into the ESXi server using my key, right?

```
       M6o5sch4                    Leedom - Cross
```

1   A. I don't remember if every single login was SSH only. I

2   just don't remember but I know on the 20th you did -- well, I

3   guess on the 15th you did.

4   Q. Well, the way it is set up, just by running the SSH command

5   it automatically uses the key, right?

6   A. When you say "it" you mean like --

7   Q. If you run SSH to log into the ESXi server you don't

8   provide any argument, it automatically uses the key; right?

9   A. I think it depends on how you have SSH set up but, like I

10   said, in this instance for this session you used your key.

11   Q. And through your forensic examination I continued to update

12   the ESXi server until I resigned in November, correct?

13   A. I don't understand. Update?

14   Q. I mean I continued to administer the server until I

15   resigned, right?

16   A. You accessed the server until -- I think the server might

17   have been turned off on -- a few days later.

18   Q. A few days later when?

19   A. I don't know if it was the 25th. I think the last entry

20   for off.log was from the 18th, I don't think it was -- was used

21   after. The session -- this April 20th session started on the

22   15th so that's why there is no entries for the 20th in there

23   but I don't believe -- there is not, like, extra logins for the

24   next six or eight months.

25   Q. No one logged into the ESXi server after April 20th?

1   A.   I would have to review the off log. I don't remember.

2   Q.   Well, you know the ESXi server was continually used after

3   this point, right?

4   A.   When you say "log in", I'm talking about the actual server

5   itself, not logging in through vSphere to make a VM, I am

6   talking about, like, using an SSHT or the root password for the

7   server to log in to the server itself.

8   Q.   Right.

9   A.   Because you said server, administrate the server. For

10   vSphere? I don't know. I don't remember.

11   Q.   Let's jump to slide 81. This e-mail specifically related

12   to the Atlassian projects, correct?

13   A.   I disagree.

14   Q.   You disagree.

15   A.   Yes.

16   Q.   What is the subject of the e-mail?

17   A.   ISB infrastructure permissions transfer.

18   Q.   And what servers were being transferred to ISB?

19   A.   All of the servers running the Atlassian products.

20   Q.   And I was removed from administrating the Atlassian

21   products at this time, right?

22   A.   I believe so from the -- from, like, Crowd. All the keys

23   were removed.

24   Q.   And the ESXi server is not an Atlassian product, correct?

25   A.   It runs the Atlassian products.

M6o5sch4   Leedom - Cross

1   Q.   It is not an Atlassian product though, right?

2   A.   No.   The VM ware of ESXi is not an Atlassian product.

3   Q.   It is a completely different server, right?

4   A.   I wouldn't say completely different.   It houses and runs

5   two of the Atlassian servers.

6   Q.   It did until April 25th, right?

7   A.   I believe so.

8   Q.   After that it didn't have any Atlassian products, right?

9   A.   I don't know if those images were still there, but yes,

10   from like a formal perspective, yes, I think they moved them

11   off.

12   Q.   And the ESXi server predated the Atlassian products,

13   correct?

14   A.   I don't remember.

15   Q.   Through your forensic examination you learned that I

16   retained access keys to multiple other servers, right?

17   A.   At this point I only remember the key on the ESX server.   I

18   know there were failed logins to the Jira server, to the Stash

19   server.

20   Q.   The Doxygen server; through your examination of the Doxygen

21   server you learned I still had my keys for that, right?

22   A.   I don't remember.

23   Q.   What about the IRC server?   Do you remember doing that

24   examination?

25   A.   I do remember doing the IRC server.   I don't remember when

1 or what the status of your keys were for that.

2 Q. But you were aware up to this point of most of the virtual

3 machines on the server I was administering, correct?

4 A. I don't know if I can speak to what you were administering

5 or what.

6 Q. There were at least 20 or so different virtual machines on

7 the ESXi server, right?

8 A. I believe so.

9 Q. And your testimony is that you don't recall if I continued

10 to administer them or you don't recall -- is that your

11 testimony?

12 A. Yeah. I don't recall, like, A, what administrative actions

13 you were performing to, like, the development servers and --

14 yeah, that's the main -- that's the main part. Like, I was

15 mostly focused on the Atlassian stuff.

16 Q. And you testified that I was logged into the ESXi server

17 when this e-mail was sent, right?

18 A. Yes. Your session began on the 15th.

19 Q. So through your examination you were aware that there were

20 multiple other systems also logged in at this time, right?

21 A. Can you explain?

22 Q. I'm sorry. I didn't hear.

23 A. Can you explain multiple other systems?

24 Q. Yes. The SSH session into the ESXi server was not the only

25 open session, correct?

M6o5sch4   Leedom - Cross

1   A.   So it is important to make the distinction of an

2   administrative session to the actual server itself using SSH

3   and what someone might have logged in with vSphere to use a

4   virtual machine. Those are different things.

5   Q.   No, I am talking specifically about SSH.

6   A.   I know that I think it might have been Jeremy's session

7   closed sometime on the 18th. Whether it was before or after

8   this e-mail I'm not sure.

9   Q.   I'm just talking about my open SSH sessions at this time.

10   How many servers were I connected to when this e-mail was sent?

11   A.   I can only speak to the ESXi server.

12   Q.   Retaining your open session to a system is not -- retaining

13   an open session to a system is normal, correct?

14   A.   It depends.

15   Q.   It depends on what?

16   A.   I mean, like, if I had an open session to a machine and

17   then there was a permission change on that exact machine, I

18   think that would be some cause for concern which is why it is

19   included here.

20   Q.   But I don't know, because I -- let me rephrase that

21   question.

22   Because I used the ESXi key I don't know that

23   permissions -- that the password has been changed, correct?

24   MR. DENTON: Objection.

25   THE COURT: Sustained.

M6o5sch4   Leedom - Cross

1   Q.   If you use an SSH key to log into a server you will not

2   know when a password is changed on the server, correct?

3   A.   Not from doing the normal SSH login process.

4   Q.   OK.

5   A.   It doesn't use the password like that.

6   Q.   Let's take a look at what is in evidence as Government

7   Exhibit 1071.   Just the subject of the e-mail.

8   A.   Do you want me to read it?

9   Q.   Just the subject.

10   A.   CMR: Transfer of equipment (especially OSB server) to OSB.

11   Q.   This is a request to transfer ownership of the ESXi server,

12   correct?

13   MR. DENTON: Objection.

14   THE COURT: Overruled.

15   A.   I don't know what the formal transfer of investment process

16   was for DevLAN or CIA property in general, but this appears to

17   be you asking what the process is for transferring the OSB

18   server, which I assume is the ESXi server, because it is called

19   OSB, so.

20   Q.   And in the e-mail it's specifically a request to transfer

21   accesses too, right?

22   A.   It just says the equipment and remove your access.

23   Q.   I'm sorry.   What was your answer?

24   A.   It says to transfer the equipment and to remove your

25   access.

M6o5sch4   Leedom - Cross

1   Q. So it is a request to transfer my accesses, right?

2   MR. DENTON: Objection.

3   THE COURT: Sustained.

4   Q. And the date of this e-mail?

5   A. It is April 21st.

6   Q. But, to your knowledge through the investigation, the ESXi

7   server was never transferred at this time, correct?

8   A. I don't know. I don't have, like, the property forms from

9   the agency. I don't see how or if a transfer occurred.

10 Q. I mean, there was no additional keys were added to the

11 authorized key file, right?

12 A. When we received it I believe your key was the only key

13 that was in there.

14 Q. I will take that down.

15   So let's talk a little bit about the ESXi access in

16 general. So you testified earlier I had my key on the ESXi

17 server, correct?

18 A. Yes.

19 Q. And that's a root key, correct?

20 A. Yes. There is only, I think, one account on there.

21 Q. The primary administrator for the server, correct?

22 A. Yes.

23 Q. And what authorization comes with the root server key?

24 A. I'm not -- can you explain a little further?

25 Q. What types of commands are root users authorized to

M6o5sch4   Leedom - Cross

1   execute?

2   A. Pretty much everything.

3   Q. Anything, right?

4   A. Yes.

5   Q. By virtue root of server key the user is permitted to

6   perform any command, correct?

7   A. Yes.

8   Q. The root key authorizes users to install programs, correct?

9   A. Yes.

10   Q. Root key authorizes the user to update the system, correct?

11   A. Yes.

12   Q. And root key authorizes the user to delete files, correct?

13   A. Yes. It will let you do pretty much any kind of

14   administrative action.

15   Q. So the root user can technically reformat or completely

16   wipe the system, right?

17   A. Yes, if they chose to do so.

18   Q. And specifically with respect to virtual machines, the root

19   key authorizes the user to create, modify, delete, snapshot,

20   revert, or do anything at all with virtual machines, right?

21   A. Yes.

22   Q. And just for clarification here, the root ESXi key does not

23   grant any privileges on the VMs themselves, right?

24   A. That's correct.

25   Q. So you can be a root user of the ESXi server and have no

M6o5sch4   Leedom - Cross

1   access to the VMs, correct?

2   A.   Yes.   That's correct.

3   Q.   The virtual machines control their own access, correct?

4   A.   They do.

5   Q.   OK.   Let's pull up slide 71 in your presentation.   Here you

6   note that the root password changed for the Confluence virtual

7   machine, correct?

8   A.   Yes.

9   Q.   And root password is the administrator password, right?

10   A.   Yes, it is.

11   Q.   But there was also a regular user account called

12   Confluence, right?

13   A.   Yes; a service account.

14   Q.   And this regular user account also allowed you to log into

15   the Confluence server, correct?

16   A.   Yes.   I don't remember the exact, like, permission string

17   for it.   It's an account that is automatically created when you

18   install Confluence.   The Confluence service uses it for things,

19   I don't know what exactly.

20   Q.   We can pull up the 1207-11, it is in evidence.   So this is

21   the file with both the users, right?

22   A.   Yes.

23   Q.   The Confluence user password was 123ABCDEF, right?

24   A.   I don't remember.

25   Q.   You don't remember the password to the Confluence system?

1   A.   No.

2   Q.   And this password was not changed though, correct?

3   A.   I don't remember. I don't look at the before and after.

4   Q.   We can look at the others. The other one is 1207-21,

5   right?

6   A.   Yes. They look to be the same.

7   Q.   It is the same, right?

8   A.   Yes.

9   Q.   And this password, even though you don't recall it, it

10   would still be reflected in the Confluence, right?

11   A.   Are you talking about in the virtual machine?

12   Q.   No. I mean, there was OSB's ESXi page on Confluence,

13   correct?

14   A.   There was a page, yes.

15   Q.   And it contained the accounts for the -- to log in,

16   correct?

17   A.   I don't remember if it had the -- I don't remember if it

18   had this password. It might have had a password for the,

19   like -- I'm trying to say the password for the user account,

20   for Confluence on disk. It doesn't necessarily have to be the

21   same as the password for the web service, kind of store it in

22   different places. I also don't ever recall seeing the

23   Confluence account ever like logged into like that.

24   Q.   OK. So you don't recall if the user name and password was

25   on the ESXi page? Is that right?

M6o5sch4   Leedom - Cross

1   A. ESXi, I don't remember what that password hash resolves to

2   so I don't remember which password that was. I know passwords

3   were stored on that page. I don't know if it is that one

4   specifically.

5   Q. OK, but you know that I had it saved -- or saved the

6   configuration of that page, correct?

7   MR. DENTON: Objection.

8   THE COURT: Sustained.

9   Q. Through your -- all right, let's pull up what is in

10   evidence as Government Exhibit 1202-3. So this is a save of

11   that server page, correct?

12   A. Yes.

13   Q. That contained the configurations for the server, right?

14   A. Yes, I think that's the page that had the passwords on it,

15   if I remember correctly.

16   Q. OK. And the Alta backups were mounted on the public/mount

17   directory, correct?

18   A. That directory does have permissions. It should be owned

19   by root.

20   Q. The mount directly -- what permissions was it mounted as?

21   A. I believe it was owned by root. I mean, the share was

22   mounted read/write but that folder on Confluence itself, I

23   believe it to be owned by root.

24   Q. But it was mounted with read access, right?

25   A. Yeah, but that doesn't affect the owner. If you are not --

1   if you logged in as the Confluence user and not the root user,

2   if you tried to access that folder I don't believe you would be

3   able to.

4   Q.   Why?

5   A.   Because of the ownership permissions of that folder.

6   Q.   Well, it doesn't matter who owns it, it matters what is the

7   access controls on the folder, right?

8   A.   The access controls on the folder would be the group that

9   owns it, which I believe was the root group.

10   Q.   I mean, you can set access controls to be -- to have anyone

11   access that?

12   A.   The root user could but not the --

13   Q.   In Linux you can configure access controls through a

14   different directory, right?

15   A.   Yes, you can.

16   Q.   So if you own a directory you can have somebody else access

17   your directory, right?

18   A.   If you change the permissions.

19   Q.   OK. Do you know what the permissions were set to on that

20   directory?

21   A.   I believe it was root root. I believe it was owned by

22   root.

23   Q.   But you don't know for sure what it is sitting here, right?

24   A.   I want to see the exhibit so I can confirm but that's what

25   I remember.

M6o5sch4   Leedom - Cross

1   Q. Was there an exhibit that listed the access controls in

2   your slide presentation?

3   A. Not in the slide presentation, no.

4   Q. But if the access controls were not set properly, a regular

5   user could log in and access that, correct?

6   A. Yeah. If the access controls were set to where a user

7   could do that, yes, they could do that.

8   Q. Next let's go on to slide 87. I just briefly want to touch

9   on this. This was sent on April 20th, correct?

10   A. Correct.

11   Q. Can you say whether I even opened or read this e-mail on

12   April 20th?

13   A. Not sitting here today.

14   Q. And the e-mail says the migration is going to take place

15   April 25th, correct?

16   A. That's what the e-mail says.

17   Q. So from April 20th to 25th there is still five days, right?

18   A. That's correct.

19   Q. I think the 20th is a Wednesday, right?

20   A. This says April 25th is a Monday, so I believe so.

21   Q. So Thursday, the 21st, Friday, the 22nd, and the weekend,

22   the server is still -- everything is going to be on the ESXi

23   server, right?

24   A. That's what this says.

25   Q. Let's take a look at slide 48. So my CIA workstation was

M6o5sch4   Leedom - Cross

1   completely intact when you found it, right?

2   A.   Yes.

3   Q.   Which means I did not reformat or wipe it before I left,

4   correct?

5   A.   Not that I could tell.

6   Q.   And have you heard of DBAN?

7   A.   Yes.

8   Q.   DBAN is used to completely wipe a drive, right?

9   A.   Yes, it is.

10   Q.   And it is basic security practice to wipe drives when you

11   finish with them, right?

12   A.   I don't know what CIA's security policy is, but in a

13   general sense if you are finished with a drive that is under

14   your control, yes, you can wipe it.

15   Q.   And through your forensic examination I had multiple copies

16   of DBAN at my desk, right?

17   A.   I believe there were some disks with DBAN. I don't

18   remember if they were found at your desk or not.

19   (Continued on next page)

20

21

22

23

24

25

M6oWsch5   Leedom - Cross

1   BY MR. SCHULTE:

2   Q. OK. I could have used DBAN to wipe the workstation, right?

3   A. Yes.

4   Q. In fact, at the very least, it would have been very easy to

5   zero the unallocated space, right?

6   A. I don't know about very easy, but that's something you

7   could have done.

8   Q. I mean the command is just copydevurandom in a file, right?

9   MR. DENTON: Objection.

10   THE COURT: Sustained.

11   (Defendant conferred with standby counsel)

12 BY MR. SCHULTE:

13 Q. What is devurandom on Linux?

14 A. So, there's a -- it's a -- we'll call it a file. If you

15 read it, it will give you a, a random output.

16 Q. So if you copy that to a file, it will write over

17 unallocated space, right?

18 A. Yes. It will -- it will store the file, and if there's

19 stuff that was there before, it will get overwritten.

20 Q. And then you unlink it with the RM command, right?

21   MR. DENTON: Objection.

22   THE COURT: Can I see counsel and everybody at

23 sidebar.

24   (Continued on next page)

25

1   (At sidebar)

2   THE COURT: Part of the reason I took a break is that

3   I think one of the jurors, juror No. 13, has been out cold for

4   at least the last 20 minutes. That, I think, is a metaphor,

5   however, for the cross here, which I just don't get.

6   What is going on? You elicit from him that it's

7   possible to erase the unallocated space, what program, what

8   command lines. It doesn't matter. No one cares. The jury

9   certainly doesn't understand or get it. You're just wasting

10   their time, my time, and losing the point. So it's not

11   effective for your purposes, and it's just a waste of time.

12   How much more cross do you have? What do you need to

13   cover?

14   MR. SCHULTE: I mean I think the point was just the

15   expertise that could be easily -- you know, this could have

16   been easily wiped. I think that's all I was trying to get out.

17   This is just a small --

18   THE COURT: The particular commands that he might use

19   to do that are not relevant.

20   MR. SCHULTE: But I mean just showing how small -- you

21   know, if you have to do, like, a long, lengthy process to do

22   it, it's different than running one command, right?

23   THE COURT: OK. How much more do you have to cover

24   here?

25   MR. SCHULTE: Want me to go check? I can go check.

1   THE COURT: No.

2   MR. SCHULTE: Like, two or three topics left.

3   THE COURT: OK. Let's move it along. You're losing

4   the jury and not making much progress here. OK? So make it

5   snappy if you can.

6   Anything that you want to raise or you want to raise?

7   Mr. Denton.

8   MR. DENTON: No.

9   THE COURT: OK. Very good.

10   (Continued on next page)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

M6oWsch5   Leedom - Cross

1   (In open court)

2   BY MR. SCHULTE:

3   Q.   Just briefly -- we'll finish this -- the point is it would

4   only take a few seconds to run these commands, right?

5   A.   Not necessarily.

6   Q.   OK. Let me rephrase that.

7   It takes a few seconds to type the command, right?

8   A.   Yes.

9   Q.   OK. And if that had happened, there would be no

10   recoverable data from the unallocated space, right?

11   A.   I can't really speak to that. You'd, you'd have to

12   completely fill the disk.

13   Q.   OK. But this was never done, right?

14   A.   I don't recall seeing any evidence of that, no.

15   Q.   OK. Let's turn to slide 83.

16   There were a ton of commands executed here to attempt to

17   review log files, correct?

18   A.   That's what it appears to be, yes.

19   Q.   And you would agree that this kind of activity is abnormal,

20   right?

21   A.   Abnormal?

22   Q.   Yes.

23   A.   Not this, not this activity. This is just viewing log

24   files.

25   Q.   Well, I guess the breadth, the number of log files and

M6oWsch5   Leedom - Cross

1   what's being reviewed is a lot here, right?

2   A. I would say this is actually pretty minimal. It's only,

3   like, four log files.

4   Q. All right. You testified on direct that I deleted log

5   files on the ESXi server, correct?

6   A. Yes.

7   Q. But none of those log files would have captured copy

8   commands, correct?

9   A. That's incorrect.

10   Q. Which one would?

11   A. Shell.log would capture copy commands.

12   Q. No. Shell.log is on the ESXi server, right?

13   A. You didn't specify which server, just copy commands in

14   general.

15   Q. OK. A copy command from Confluence wouldn't have been

16   logged in those ESXi log files, right?

17   A. The command itself, no.

18   Q. The bigger issue is, turning to slide 117, can you tell me

19   what's wrong with what you claim to be deletions here?

20   A. A lot of deletions.

21   Q. But the command executed, RM, does not wipe the log, right?

22   A. It deletes the file.

23   Q. Well, this command unlinks the file, right?

24   A. Yes.

25   Q. OK. There's no slash S argument to RM, right?

M6oWsch5   Leedom - Cross

1   A.   Well, there's -- no.

2   Q.   And there's no SRM command, right?

3   A.   I -- I don't think SRM was available. I'm actually not

4   even sure dash S is available on -- on ESX or not.

5   THE COURT: Mr. Leedom, can you translate what those

6   terms mean.

7   THE WITNESS: Yeah. What Mr. Schulte's describing are

8   flags that you pass to these commands to explicitly, like,

9   overwrite that unallocated space for the file, like, we call a

10   secure erase. I'm not sure what -- I'm not sure if SRM's

11   available on ESX; I don't think it is, and I'm not sure if the

12   S flag or RM either. But no, those flags are not present here.

13   BY MR. SCHULTE:

14   Q.   OK. But if someone -- if you were attempting to cover your

15   tracks, this is what you would use, right?

16   A.   I disagree. I've seen it just like this plenty of times.

17   Q.   The files themselves are still available, though, right?

18   A.   The content is -- is -- could potentially be there at a

19   later date.

20   Q.   OK. Are you familiar with services?

21   A.   In what way?

22   Q.   Well, in Linux, what's called daemons?

23   A.   Yes.

24   Q.   OK. And ESXi runs daemons for the VMs, right?

25   A.   Yes, I believe there's one that manages the VMs.

1   MR. SCHULTE: OK. I just want to show the witness

2   what's marked defense exhibit 1204-2 -- sorry, 1204-1.

3   Q. You're familiar with vSphere, correct?

4   A. To some extent, yes.

5   Q. And ESXi, right?

6   A. Yes.

7   Q. Were you able to review the contents of any of the log

8   files?

9   A. Yes.

10   Q. The content -- I'm sorry -- of the unlinked log files?

11   A. I don't believe -- I think there was some file side from

12   shell.log, but I don't believe there was any from the others.

13   Q. OK. And Dave and Jeremy are the ones who came in on April

14   16, 2016, to take the snapshot of the Confluence VM, correct?

15   A. Like I said, I don't -- I think Jeremy logged in to the

16   ESXi server.

17   Q. OK.

18   A. ISB.

19   Q. ISB. But neither of them had any experience in Linux or

20   ESXi, right?

21   A. I do not know.

22   Q. OK. Can you say whether their actions caused some daemons

23   to crash on that day?

24   A. I don't recall.

25   THE COURT: Can we take this document off the screen,

M6oWsch5   Leedom - Cross

1   please.

2   MR. SCHULTE: All right.

3   Q. Can you say whether or not log files were corrupted on that

4   day?

5   A. I don't -- I don't remember any -- I can't really speak to

6   the actions they took other than changing the passwords.

7   Q. OK. But through your knowledge with system administration,

8   if there's a problem with the host service running the VMs,

9   that could cause problems for all the VMs, correct?

10   A. Depending on how the host service operates and the type of

11   errors, it could potentially. I --

12   Q. OK.

13   A. -- kind of have to say as a theoretical, but --

14   Q. And you don't typically want to restart a service like that

15   because it will restart all the virtual machines, right?

16   A. It could. I'm not sure exactly of the, like, specific

17   effects of restarting the -- I think the VMware host service,

18   ESXi server.

19   Q. OK. But at the time you know that there were at least 20

20   virtual machines on the ESXi server, right?

21   A. Yes. I don't remember exactly how many were running at the

22   time, but there were multiple machines on there.

23   Q. OK. So in case of any problems, the best option would be

24   to disable and fix the sole VM causing trouble for the daemon,

25   right?

1   A.   It depends.

2   MR. SCHULTE: OK. Just going to publish what's your

3   slide 111 here.

4   Q.   Did you notice any pattern at all to your analysis of the

5   log files?

6   A.   Not sure I'm following. Aside from you deleting activity

7   after performing activity?

8   Q.   All right. The core VM 25 technique --

9   A.   I'm sorry?

10 Q.   Did you notice that?

11 A.   I don't know what that is.

12 Q.   OK. So, at 5:55 to 5:57 p.m. was two minutes, right?

13 A.   Yes.

14 Q.   OK. And those are core ESXi system files, right?

15 A.   I'm sorry. But the log files that were deleted between

16 those two minutes?

17 Q.   Yeah.

18 A.   I believe so. I don't know exactly which ones those were,

19 but --

20 Q.   OK. I think we can pull it up.

21   5:57, those are core ESXi files, right?

22 A.   In the top?

23 Q.   Yeah.

24 A.   Yeah, vmkernel is.

25   MR. DENTON: I'm sorry, your Honor. Since our screen

1   isn't working, it would just help if we could identify what

2   we're looking at.

3   THE COURT: Page 121 of the slide deck.

4   MR. DENTON: Thank you.

5   THE COURT: We're trying to get an IT person up to see

6   if he can fix the screens, and here he is.

7   And could the witness just repeat.

8   THE WITNESS: Yes. I said vmkernel.log.

9   THE COURT: And when you refer to core ESXi files,

10   what do you mean by that?

11   THE WITNESS: So, what I assume it to mean is this

12   would be one of the more important log files that contains,

13   like, an abundance of information about the system.

14   BY MR. SCHULTE:

15   Q. OK. And going up to slide 117, this was 5:55, right?

16   A. Yes.

17   Q. And these are also core ESXi files, right?

18   A. Yeah, they're, they're all -- they're all log files for

19   ESXi.

20   Q. OK. So just going back to slide 111, again, so 5:55 to

21   5:57 is two minutes, right?

22   A. Yes.

23   Q. And then 5:57 to 6:16 is 20 minutes, right, thereabouts?

24   A. Yes.

25   Q. 6:16 to 6:38 is 20 minutes, right?

1   A.   22 minutes.

2   Q.   6:38 to 6:56 is 20 minutes, right?

3   A.   About.

4   Q.   And then it ends as it began, two minutes, 6:56 to 6:58,

5   right?

6   A.   Yes.

7   Q.   OK. And again, 116, 117 is showing the ESXi files, and

8   then 121 is showing ESXi files, right?

9   A.   Yes.

10   Q.   122, ESXi files, right?

11   A.   Yes.

12   Q.   And then precisely 20 minutes later, 127, it's another ESXi

13   file, right?

14   A.   Yes.

15   Q.   129 is -- this is showing the Confluence data stored in the

16   ESXi system, right?

17   A.   Yes, this is the folder where the Confluence virtual

18   machine lives.

19   Q.   OK. So 6:38, this is showing the file in the Confluence

20   directory on the ESXi server, right?

21   A.   Yes.

22   Q.   OK. And then 20 minutes later, on slide 132, some of the

23   same types of files, right?

24   A.   Yes.

25   Q.   136, again, right?

M6oWsch5   Leedom - Cross

1   A.   This is back in the, the main ESXi server, log folder?

2   Q.   No. The first command.

3   A.   Rmvmware.log?

4   Q.   Yes.

5   A.   That's in the main log folder for ESXi.

6   Q.   All right. But does the timing, the timing of this and the

7   actions performed indicate to you the core VM 25 technique

8   here?

9   A.   Like I said, I don't know what that is.

10   Q.   OK. Let's go to slide 124. I just want to cover this

11   briefly. Your testimony is that I deleted log files on the

12   ESXi server, right?

13   A.   Yes.

14   Q.   Most of the files are in unique locations on the ESXi

15   server, right?

16   A.   Yes.

17   Q.   And then quoting from your direct, I searched for client

18   logs on the ESXi server, right?

19   A.   Yes.

20   Q.   OK. And were you briefed on my technical training and

21   experience through your investigation?

22   A.   Not, like, explicitly. I knew you were a developer.

23   That's really the extent of it.

24   MR. SCHULTE: OK. I want to show what's in evidence

25   as Government Exhibit 1114.

M6oWsch5   Leedom - Cross

1   Q.   And this was just my approved résumé, correct?

2   A.   I can't speak to its approval. This appears to be a résumé

3   with your name on it.

4   Q.   All right. So, from the bottom, I worked at IBM as a

5   system administrator overseeing a test lab with over 900

6   machines, right?

7   MR. DENTON: Objection.

8   THE COURT: Sustained.

9   Let's move on, Mr. Schulte. Take this down, please.

10   MR. SCHULTE: OK.

11   Q.   On your final slide you show the eighth floor vaults locked

12   at 7:07, right?

13   A.   I don't remember the exact floor. I don't know if you can

14   pull up the exhibit or not.

15   Q.   OK. I can pull it up.

16   A.   Yes, I believe 8W would be the eighth floor. I believe.

17   Q.   And the CIA maintains surveillance video, correct?

18   A.   I don't know what their, like, physical security retention

19   stuff is.

20   Q.   You were at the building, correct?

21   MR. DENTON: Objection.

22   THE COURT: Sustained.

23   BY MR. SCHULTE:

24   Q.   So through your investigation, you didn't receive any video

25   surveillance from the CIA?

M6oWsch5   Leedom - Cross

1   A. I -- I personally did not. I don't know -- like I said, I

2   can't really speak to that.

3   Q. OK. So, the last thing, just to go through, showing what's

4   in evidence as Government Exhibit 111. And you're familiar

5   with the layout, correct?

6   A. Very rudimentarily. I've seen this diagram before, but I

7   do not -- I wouldn't be able to tell you, like, who or what was

8   where.

9   Q. OK.

10   A. I could say that, yes, this does appear to be the building.

11   That's about as far as I think I can go, unfortunately.

12   Q. Because you were never on the -- you never went through

13   these eighth or ninth floors?

14   A. I've been to those floors, but not, like, for any extended

15   period of time or even in any kind of. Like, investigative

16   capacity really.

17   Q. OK. Just going to show now the badge records, Government

18   Exhibit 105, on page 13, for April 20, and I just want to

19   highlight, this one here is showing an attempted entry at 1745,

20   which is 5:45, on 8W53A, correct?

21   A. That appears to be the line in the log.

22   Q. OK. And 8W53A --

23   (Defendant conferred with standby counsel)

24   MR. SCHULTE: I think this is a problem with the

25   exhibit.

1   Does the government have the updated 111, by chance?

2   MR. DENTON: We do, your Honor.

3   THE COURT: All right. Why don't we pull that up,

4   please.

5   Mr. Schulte, Mr. Leedom indicated he's unfamiliar with

6   the particulars of this exhibit, so I'm not sure what you're

7   attempting to do here.

8   MR. SCHULTE: Yeah, I think just the --

9   THE COURT: Just ask a question, please.

10   MR. SCHULTE: OK. If we can zoom in on the left side.

11   Yeah, if we can zoom in to the numbers there.

12   Q. So here -- I guess it's hard to see -- do you see in the

13   middle there the 8W53A, right above the -- it says kiosk and to

14   the right is electrical room, 8W75?

15   A. Is it that door?

16   Q. Yes. It's up a little bit.

17   A. It's very hard to read.

18   MR. SCHULTE: I guess there's no way to zoom in on

19   that.

20   Q. Do you see it's 8W53A there?

21   A. I can't -- I see a three. I think that's the best I can

22   really -- I can do, unfortunately.

23   THE COURT: All right. Let's move on, Mr. Schulte, I

24   think.

25   MR. SCHULTE: OK. I think this --

1   THE COURT: It's in evidence. You'll be able to make

2   arguments from it later if you wish, but given that the witness

3   has said he's not familiar with this, I'm not sure there's much

4   more you can do with this here.

5   MR. SCHULTE: OK.

6   (Defendant conferred with standby counsel)

7   MR. SCHULTE: OK. No further questions at this time.

8   THE COURT: All right.

9   Redirect.

10   REDIRECT EXAMINATION

11   BY MR. DENTON:

12   Q. Good afternoon, Mr. Leedom.

13   A. Good afternoon.

14   Q. This morning, Mr. Leedom, Mr. Schulte asked you some

15   questions about whether material had been deleted from his CIA

16   workstation. Do you remember that?

17   A. Yes.

18   Q. And you responded by referring to a host. Do you remember

19   that?

20   A. That's correct.

21   Q. What computer were you referring to as the host?

22   A. That's that E0001, his DevLAN workstation.

23   Q. And what operating system was that running?

24   A. Windows.

25   Q. Was the defendant also running a virtual machine on that

1   computer?

2   A. Yes.

3   Q. Now, Mr. Schulte asked you a number of questions about

4   something he referred to as a transcript file. Do you remember

5   that?

6   A. Yes, I do.

7   Q. Did you find any actual transcript files on Mr. Schulte's

8   virtual machine?

9   A. No.

10   MR. DENTON: Ms. Cooper, if we could put up Government

11   Exhibit 1703 and go to page 117.

12   Q. Mr. Leedom, where did you find the files that Mr. Schulte

13   kept calling transcript files?

14   A. They were all in unallocated space.

15   Q. Did you draw any conclusions about what happened to those

16   files from the fact that you found them in unallocated space?

17   A. They'd been deleted.

18   Q. Now, Mr. Schulte also asked you a series of questions about

19   whether you found a copy command in these files. Do you

20   remember that?

21   A. Yes.

22   Q. And in particular, a copy command with respect to the

23   Altabackups files, do you remember being asked those questions?

24   A. Yes.

25   Q. Where are the commands that we've been looking at that

M6oWsch5   Leedom – Redirect

1   Mr. Schulte showed you being run?

2   A.   Like what's on this slide right now?

3   Q.   Yes.

4   A.   So, these commands are all being run on the ESXi server.

5   Q.   Did the ESXi server have access to the Altabackups

6   directly?

7   A.   No.

8   Q.   Would you need access to the Altabackups directly to be

9   able to copy files from them?

10   A.   Yes.

11   Q.   Where were the Altabackups mounted directly?

12   A.   To the Confluence VM.

13   Q.   Did you find any log of the defendant running a copy

14   command in the Confluence VM to copy the Altabackup files?

15   A.   No.

16   Q.   Why not?

17   A.   We couldn't, because any log files from that VM were

18   deleted after the reversion.

19   Q.   And why were they deleted after the reversion?

20   MR. SCHULTE: Objection.

21   THE COURT: Overruled.

22   A.   Because once you do that reversion, everything that --

23   anything that would have been typed into that machine during

24   that time period would get erased.

25   Q.   Let's talk a little bit about snapshots and reversions for

1   a moment, Mr. Leedom.

2   MR. DENTON: Ms. Cooper, could we go to page 68 of

3   Government Exhibit 1703.

4   Thank you.

5   Q. Mr. Leedom, Mr. Schulte asked you some questions about

6   whether you learned that snapshots and reversions were

7   commonplace. Do you remember that?

8   A. Yes.

9   Q. How many snapshots were taken of the Confluence virtual

10   machine?

11   A. Three, just like here.

12   Q. Is that the total number that were taken?

13   A. No.

14   Q. How many were taken?

15   A. Four, in total.

16   Q. What happened to the third one?

17   A. It was deleted.

18   Q. By whom?

19   A. Mr. Schulte.

20   Q. Mr. Schulte also asked you some questions about SSH keys

21   just a moment ago. Do you remember that?

22   A. Yes.

23   Q. He asked you what SSH keys authorize?

24   A. Yes.

25   Q. Whether they authorize making changes to virtual machines,

1   right?

2   A.   Yes.

3   Q.   What do you mean when you say it authorizes that?

4   A.   So, when you store an SSH key, it's associated with a,

5   like, a certain user account; in this case, the administrator

6   user.

7   Q.   On April 20, 2016, did the CIA allow Mr. Schulte to make

8   changes to the Confluence virtual machine?

9   MR. SCHULTE: Objection.

10   THE COURT: Overruled.

11 A.   When you say allow, do you mean did he have permission to,

12 or --

13 Q.   Is there a distinction in this context between having

14 permission and being authorized through an SSH key?

15   MR. SCHULTE: Objection.

16   THE COURT: Overruled.

17 A.   So, if your, if your key is there, then you can, you know,

18 physically log in to it and make changes.   The only thing

19 stopping you would be if your key wasn't there.

20 Q.   Is that different from being authorized to by policy?

21 A.   Yes.

22 Q.   Now, Mr. Schulte asked you a number of questions about

23 hypothetical possibilities with respect to the DevLAN system,

24 right?

25 A.   Yes.

1   Q. As a general matter, what level of permissions were

2   required to access the Atlassian backups?

3   A. You'd need administrator permissions.

4   Q. Now, with respect to some of those hypotheticals,

5   Mr. Schulte asked you about foreign adversary penetrations of

6   DevLAN. Do you remember that?

7   A. Yes.

8   Q. Was that a focus for you when you began your investigation?

9   A. It was.

10   Q. Was that something that you looked for evidence of?

11   A. Yes.

12   Q. Did you find any evidence of that?

13   A. No.

14   Q. Mr. Schulte asked you some hypothetical questions about

15   things that Dave and Jeremy might have done. Do you remember

16   that?

17   MR. SCHULTE: Objection.

18   THE COURT: Overruled.

19   A. Yes.

20   Q. Were Dave and Jeremy also administrators of the system?

21   A. Yes, they were.

22   Q. As part of your investigation, did you focus on whether

23   administrators other than Mr. Schulte might have taken this

24   data?

25   A. Yes.

M6oWsch5   Leedom - Redirect

1   Q. Did you include Dave and Jeremy in that?

2   A. Yes.

3   Q. Did you find any evidence that they had done that?

4   A. No.

5   Q. With respect to the other hypotheticals that Mr. Schulte

6   asked you, when --

7   MR. SCHULTE: Objection to characterization.

8   THE COURT: Overruled.

9   BY MR. DENTON:

10   Q. Did you find any evidence of these theoretical

11   possibilities?

12   A. No.

13   Q. He also asked you at various points to focus on single

14   pieces of your analysis. Do you remember that?

15   A. Yes.

16   Q. When conducting forensic analysis, do you focus on single

17   items of evidence in isolation?

18   A. It's about the whole picture.

19   Q. Why is that?

20   A. Just about anything taken in isolation, out of context,

21   is -- it's not going to provide the necessary information to

22   understand it.

23   Q. So let's take an example of that.

24   MR. DENTON: Ms. Cooper, if we could go back to page

25   117 of Government Exhibit 1703.

M6oWsch5   Leedom - Redirect

1   Q. Do you remember Mr. Schulte asked you some questions about

2   what constituted normal system administrator activity?

3   A. Yes.

4   Q. Taken in context, is what is shown in Government Exhibit

5   1203-29 normal system administrator activity?

6   A. No.

7   Q. Why not?

8   A. Because the amount of logs and type of logs that are being

9   deleted here, you -- you just wouldn't do it.

10   Q. In your experience, what is it consistent with?

11   A. Activity of trying to --

12   MR. SCHULTE: Objection.

13   THE COURT: Overruled.

14   A. Activity of trying to cover your tracks, trying to, trying

15   to, you know, clean up after yourself, trying to inhibit

16   others' ability to see what happened at the time these log

17   files stored information.

18   MR. DENTON: If we could go to page 139, Ms. Cooper.

19   Q. And Mr. Schulte also asked you some questions about whether

20   using snapshots and reversions was normal system administrator

21   activity. Do you remember that?

22   A. Yes.

23   Q. Was the pattern of reversions and snapshots by Mr. Schulte

24   on April 20 consistent with normal administrator activity?

25   A. No.

1   Q.   How was it inconsistent with that?

2   A.   I mean we can even just look at the Confluence VM. There

3   were four snapshots taken over the course of a couple years.

4   And this had never happened before, this snapshot reversion for

5   this, especially within, like, a one-hour time frame. It's not

6   something that -- you know, it's not something that happened

7   every Friday at 1:00. This is an instance, a single instance

8   of something outside the normal.

9   MR. DENTON: And then we could go to the next page,

10 page 140.

11 Q.   What was outside the normal about Government Exhibits

12 1207-27 and 1207-30?

13   MR. SCHULTE: Objection.

14   THE COURT: Overruled.

15 A.   All these access times are the same and almost identical to

16 the date created and date modified. For these two entries that

17 are highlighted, for the March 3 backup, the access time is

18 different. It's on April 20.

19 Q.   And is that a fact that you considered together with other

20 parts of the forensic evidence that you found in this case?

21 A.   Absolutely.

22 Q.   And did that lead to the conclusions that you drew?

23 A.   Yes.

24 Q.   What conclusion was that?

25 A.   That the defendant copied these backup files while the

1   Confluence VM was in that reverted state.

2   Q. And as a result of the defendant's activities, were you

3   able to recover the specific command to copy those files?

4   A. No.

5   MR. DENTON: No further questions, your Honor.

6   THE COURT: Any brief recross?

7   RECROSS EXAMINATION

8   BY MR. SCHULTE:

9   Q. Mr. Denton asked you about the level of permission needed

10   to access the Altabackups, correct?

11   A. Yes.

12   Q. But the access controls were lost before you were able to

13   recover them, correct?

14   A. To some extent they were, yes.

15   Q. I mean you never recovered any access controls for the

16   Altabackup, correct?

17   A. I think we had to, like, for the folder, like, you had to

18   be root to access the folder. But all of the allow listing, IP

19   address information for the config, we didn't have that.

20   Q. OK. So sitting here today, you don't know what the

21   permissions on those allow and deny lists were, correct?

22   A. Correct.

23   Q. Mr. Denton asked you whether you investigated Dave and

24   Jeremy, correct?

25   A. Yes.

M6oWsch5   Leedom - Recross

1   Q. And just to confirm, Dave C. saved a copy of Stash on his

2   home directory, correct?

3   A. Yes. We looked at it.

4   Q. And his home directory was public, correct?

5   A. I don't know the, the permissions for that home directory.

6   I -- I think from previous statements from Dave, he said that

7   it had -- he had, like, locked it down. But I don't remember

8   exactly what the -- what the permissions are exactly. But I

9   just know in some previous statements I think that that's what

10   he'd said.

11   Q. Well, we saw defense exhibit 1201 earlier and it doesn't

12   show any access list controls directory on that, right?

13   A. I think that was just for the, like, root directories. I

14   don't think that list showed every single person's home folder.

15   Because you could change the permissions on your home folder

16   even though the people could see, like -- like, they could even

17   see your folder but may not be able to go into your folder

18   based on the permissions.

19   Q. But those permissions would have been logged in the

20   exhibit, right, for all the access controls?

21   A. I don't know how large that, that exhibit was that we

22   looked at. That may have just been an exhibit of, like, the

23   top-level shares.

24   Q. So your testimony is that you don't know what access his

25   home directory was set to?

M6oWsch5   Leedom - Recross

1   A.   Sitting here today, I don't -- I don't recall the exact

2   permissions. I just know -- I think hearing from Dave that

3   they were -- they were changed. And I'm sure I reviewed them

4   at some point in the past, but I don't remember exactly right

5   now.

6   Q.   OK. But Dave C. is the same individual who lost the hard

7   drive with Stash on it too, right?

8   MR. DENTON: Objection.

9   THE COURT: Sustained.

10   Next line, please.

11   BY MR. SCHULTE:

12   Q.   OK. And you said the snapshot reversion was outside the

13   normal, correct?

14   A.   Yes.

15   Q.   But it happened at 5:35 p.m. on a weekday, correct?

16   A.   I believe so.

17   Q.   And people were still working, correct?

18   THE COURT: All right. Sustained. Asked and

19   answered.

20   Any new questions based on the redirect, Mr. Schulte?

21   BY MR. SCHULTE:

22   Q.   The transcript files you talked about with Mr. Denton,

23   about the log-in or copy command, but if a log-in to the VM or

24   copy command had been run, you would have seen that in the

25   transcript files, correct?

M6oWsch5   Leedom - Recross

1   A.   It really depends.

2   Q.   Depends on what?

3   A.   Well, A, if those are even actually transcript files, and

4   B, like, if all of the -- if they were there, if -- if that

5   activity was even stored in one was available. I mean all I

6   can speak to is the available evidence, and there was nothing

7   in there showing that.

8   Q.   OK. But those transcript files are from my CIA

9   workstation, correct?

10   A.   Yes.

11   Q.   And they're showing log-in -- they're showing commands

12   being run on a remote server, correct?

13   A.   Yes.

14   MR. SCHULTE: OK. No further questions.

15   THE COURT: All right. Can we let Mr. Leedom go?

16   MR. DENTON: We can, your Honor.

17   THE COURT: All right. Mr. Leedom, you may put your

18   mask back on and step down. You're excused.

19   (Witness excused)

20   THE COURT: Mr. Denton, next witness.

21   MR. LOCKARD: The government calls Michael Berger.

22   MICHAEL BERGER,

23   called as a witness by the government,

24   having been duly sworn, testified as follows:

25   THE COURT: You may proceed, Mr. Lockard.

1   MR. LOCKARD: Thank you, your Honor.

2   DIRECT EXAMINATION

3   BY MR. LOCKARD:

4   Q. Good afternoon, Mr. Berger.

5   A. Good afternoon.

6   Q. Who is your employer?

7   A. I work for the Federal Bureau of Investigation.

8   Q. And what is your position with the FBI?

9   A. I'm a computer scientist, currently assigned to the New

10   York field office.

11   Q. For how long have you been a computer scientist with the

12   FBI?

13   A. Approximately ten years.

14   Q. Do you have any degrees relating to computer science?

15   A. Yes, I do.

16   Q. And what degrees are those?

17   A. I have a bachelor's of science in computer science, I have

18   a master's of science in computer forensics, and a master's of

19   science in computer science.

20   Q. You said you have a master's in computer forensics?

21   A. That is correct.

22   Q. What is computer forensics?

23   A. Computer forensics is the area of study that deals with

24   applying forensic science to looking through digital evidence.

25   Q. Do you have any other professional responsibilities

M6oWsch5   Berger - Direct

1 relating to the field of computer science?

2 A. Yes, I do.

3 Q. And what is that?

4 A. I also teach digital forensics.

5 Q. And where do you teach?

6 A. At the school of engineering at New York University.

7 Q. For how long have you taught digital forensics at NYU?

8 A. About three years.

9 Q. And we talked about computer forensics. What is digital

10 forensics?

11 A. Digital forensics is just the more modern term for computer

12 forensics. You can think of it as the overarching term that

13 would include computer forensics, network forensics, mobile

14 device forensics, things like that.

15 Q. Turning back to your responsibilities as an FBI computer

16 scientist, are you currently assigned to any particular group

17 within the FBI?

18 A. Yes, I am.

19 Q. What group are you assigned to?

20 A. I'm assigned to the cyber branch of the New York field

21 office, specifically cyber squad CY1.

22 Q. What types of cases does the branch that you're assigned to

23 generally investigate?

24 A. Cyber branch generally investigates what are known as

25 computer intrusions, basically a fancy way of saying hacking,

1   someone getting unauthorized access to a computer that does not

2   belong to them.

3   Q. And your squad in particular, does it investigate a

4   particular type of cyber crimes?

5   A. Yes.

6   Q. What do you typically investigate?

7   A. Complex national security-based intrusions.

8   Q. Have you participated in professional training related to

9   computer science and computer forensics?

10   A. Yes.

11   Q. And what types of trainings have you participated in?

12   A. I've taken both trainings internal to the FBI as well as

13   external vendor-provided trainings.

14   Q. Have you provided professional training to others?

15   A. Yes.

16   Q. Can you describe what type of professional training you've

17   provided to others?

18   A. Within the FBI I've provided internal trainings to groups

19   of people or sometimes my squad or sometimes the entire cyber

20   branch.

21   Q. Mr. Berger, are you familiar with the FBI's CAT team?

22   A. Yes, I am.

23   Q. And what is the CAT team?

24   A. It's the cyber action team.

25   Q. And I think we heard a little bit about that from

M6oWsch5   Berger - Direct

1   Mr. Leedom's testimony. What kind of work does the CAT team

2   do?

3   A.   So, the CAT team is the FBI's headquarters-based incident

4   response team. They can respond both domestically and

5   internationally to very significant cyber intrusion incidents

6   or any other investigations that have a high level of technical

7   complexity.

8   Q.   And do you have a role with the CAT team?

9   A.   I do.

10   Q.   What is your role?

11   A.   I'm a member of the team.

12   Q.   For how long have you been a member of the CAT team?

13   A.   About six years.

14   Q.   Have you participated, in your career as an FBI computer

15   scientist and a member of the CAT team, in investigations of

16   computer hacking?

17   A.   Yes.

18   Q.   Have you participated in investigations of insider threats?

19   A.   Yes.

20   Q.   In your investigations, have you applied any kind of

21   specialized analyses?

22   A.   Yes, I have.

23   Q.   What kinds of specialized analyses have you applied in

24   those investigations?

25   A.   I've conducted traditional disk forensics, looking at

1   forensic images on hard drives from computers. I've also

2   conducted memory analysis, where the contents of volatile

3   computer memory is captured and then analyzed. I've analyzed

4   log files. I've reverse engineered malware, things along those

5   lines.

6   Q. And Mr. Berger, have you been qualified as an expert in

7   court proceedings in the past?

8   A. Yes, I have.

9   MR. LOCKARD: Your Honor, the government offers FBI

10   Computer Scientist Michael Berger as an expert in the subject

11   of computer science, computer forensics, and digital forensics.

12   THE COURT: Any objection?

13   MR. SCHULTE: No objection.

14   THE COURT: All right. Received.

15   Ladies and gentlemen, you'll recall my instructions a

16   few days ago about what an expert witness is and may testify

17   to. Those instructions govern here, and as I told you, I'll

18   give you additional instructions on that score at the

19   conclusion of the case.

20   Mr. Lockard, you may proceed.

21   MR. LOCKARD: Thank you, your Honor.

22   Q. Are you familiar with an investigation relating to the

23   WikiLeaks Vault 7 release?

24   A. Yes, I am.

25   Q. When did you first become involved in that investigation?

M6oWsch5   Berger - Direct

1   A.   Approximately the middle of March 2017.

2   Q.   And approximately how long after the first of the Vault 7

3   releases was that?

4   A.   I believe it was about one or two weeks.

5   Q.   And broadly speaking, what was your role in the

6   investigation?

7   A.   My role was to provide digital forensics assistance with

8   some of the evidence that was recovered at the defendant's

9   apartment.

10   Q.   And what other roles did you play in the investigation as

11   time went on?

12   A.   Throughout the investigation, I also performed analysis on

13   some of the data that was disclosed by WikiLeaks in comparing

14   it to data that was retained by the CIA in their internal

15   systems.

16   Q.   Broadly speaking again, what types of digital evidence did

17   you review in your role in the investigation?

18   A.   So, I reviewed information provided by the CIA from the

19   DevLAN system interpreting the form of database backup files.

20   I reviewed disk images that were obtained from the defendant's

21   apartment. I also looked at data provided by service providers

22   pertaining to the defendant's actions.

23   Q.   In your work as an FBI computer scientist, have you used a

24   computer user's online activities or computer activities as

25   part of your investigation?

M6oWsch5   Berger - Direct

1   A.   Yes.

2   Q.   And how does the user's activity inform your forensic

3   analysis and conclusions?

4   A.   Depending on what those activities were, they may show an

5   indication of different types of techniques that the person

6   might have been researching or looking up, and those would

7   correlate to possibly evidence of those techniques being found

8   on the evidence provided.

9   Q.   Did your review and analysis of the categories of evidence

10   that you describe include the application of some of the

11   specialized analytical techniques that you described earlier?

12   A.   Yes.

13   Q.   So, Mr. Berger, do you have in front of you a binder with

14   Government Exhibit 1704 inside of it?

15   MR. LOCKARD: Ms. Cooper, if we could show Mr. Berger

16   the first page of Government Exhibit 1704.

17   Q.   Mr. Berger, are you familiar with what's shown here?

18   A.   Yes, I am.

19   Q.   Did you participate in its preparation?

20   A.   Yes.

21   Q.   Would referring to Government Exhibit 1704 assist you in

22   explaining your methodology, some of the relevant evidence, and

23   the conclusions that you drew?

24   A.   Yes.

25   MR. LOCKARD: Your Honor, we would request permission

1   to publish 1704 as a demonstrative exhibit.

2   THE COURT: Any objection?

3   MR. SCHULTE: Yes. Same objection to the other one.

4   THE COURT: All right. Overruled.

5   You may display it.

6   Ladies and gentlemen, again, for the moment at least,

7   this is not being admitted into evidence. It's just a

8   demonstrative, an aid to allow you to help understand the

9   witness's testimony. It's the witness's testimony, unless and

10   until this is admitted as an exhibit, it is only the witness's

11   testimony that is the evidence.

12   You may proceed.

13   MR. LOCKARD: Thank you, your Honor.

14   Q. Mr. Berger, are you familiar with the organization known as

15   WikiLeaks?

16   A. Yes, I am.

17   Q. I'd like to turn to page 54 of your presentation. In the

18   course of your investigation, have you reviewed the WikiLeaks

19   site?

20   A. Yes, I have.

21   MR. SCHULTE: Objection.

22   THE COURT: Overruled.

23   MR. LOCKARD: Could we turn to the next page, please,

24   55.

25   Q. And does this display a portion of the WikiLeaks website?

1   A.   Yes, it does.

2   MR. LOCKARD: Could we turn to page 56, please.

3   Q.   What's shown here?

4   A.   This is a screenshot of the portion of the WikiLeaks

5   website that specifically details how to submit content to

6   WikiLeaks.

7   Q.   And during what time period was this particular version of

8   the WikiLeaks website available?

9   A.   This was made available on WikiLeaks' website on April 23

10   of 2016.

11   THE WITNESS: Can we turn to page 57, please.

12   Q.   What's shown here in the URL of this version of the

13   WikiLeaks site?

14   A.   So, in the URL, you can see that the WikiLeaks.org website

15   could access from archival copy created on 2016 -- April 23 of

16   2016, and it was accessed by the site in the beginning,

17   web.archive.org, also commonly referred to as the Wayback

18   Machine.

19   Q.   And is the Wayback Machine a resource that you have used in

20   the course of your investigations as a computer scientist?

21   A.   Yes.

22   Q.   And is it a resource that's been used more generally in

23   cyber investigations at the FBI?

24   A.   Yes.

25   MR. LOCKARD: If we could turn to page 58.

M6oWsch5   Berger - Direct

1   Q. So in this version of the WikiLeaks website available in

2   April of 2016, did WikiLeaks provide any instructions or advice

3   to potential leakers?

4   A. Yes.

5   MR. SCHULTE: Objection.

6   THE COURT: Overruled.

7   BY MR. LOCKARD:

8   Q. What instructions did WikiLeaks provide?

9   A. So, they list several pieces of information on this site.

10 As depicted in the screenshot here, they also recommend the use

11 of two different utilities, TOR and Tails.

12   MR. LOCKARD: And we can move to slide 59.

13 Q. Is that what's described in this portion of the website?

14 A. Yes.

15   MR. LOCKARD: Move to slide 60.

16 Q. Mr. Berger what did WikiLeaks say about the TOR service?

17 A. They describe TOR as an encrypted anonymizing network that

18 makes it hard to intercept communications.

19 Q. Are you familiar with the TOR network?

20 A. Yes, I am.

21   MR. LOCKARD: Turn to page 61, please.

22 Q. Can you describe what is TOR and how does it work?

23 A. So, TOR is set up as kind of how it was just described, an

24 encrypted anonymizing network. There are many people out there

25 that run what are called TOR nodes. They set their computer up

1   as a TOR node, and it connects into TOR network.

2   If a user, in this case shown on the demonstration slide,

3   Alice, wants to use the TOR network, she would use the TOR

4   client on her computer that would connect through the TOR

5   network. The TOR network would then establish a circuit

6   through the TOR network going between several different TOR

7   nodes until eventually it would emerge from what we see

8   referred to as a TOR exit node, and Alice's traffic would then

9   emerge onto what we know as the regular internet.

10   If at any point anyone looked at any of the communications

11   between Alice and the first TOR node or between any of the

12   other TOR nodes, they would not be able to identify any

13   discerning information or see the content of that data being

14   transferred.

15   MR. LOCKARD: Ms. Cooper, can we please turn to page

16   74.

17   Q. Mr. Berger, in your role in the investigation, did you find

18   evidence of the defendant's use of TOR?

19   A. Yes.

20   Q. What are we looking at on page 74, displaying Government

21   Exhibit 1401-12?

22   A. This is a screenshot from a Linux virtual machine that was

23   found on the desktop computer in the defendant's apartment.

24   Q. So, we've heard a little bit about virtual machines in the

25   course of the trial testimony, but could you please just

1   summarize -- again, very briefly -- what is a virtual machine?

2   A. So, a virtual machine is essentially a way to run one or

3   more additional computer systems within a physical computer

4   system. It allows for running different operating systems.

5   For an example, you could have a Windows computer and you want

6   to run a Linux system without actually getting a second,

7   additional computer.

8   Q. And when a user is running a virtual machine on their

9   desktop, are they able to switch back and forth between the

10   virtual machine and other applications?

11   A. Yes.

12   Q. Are you able to run more than one virtual machine at a

13   time?

14   A. Yes.

15   Q. What's shown here in the circled icon on the defendant's

16   virtual machine desktop?

17   A. That is the icon for the TOR browser.

18   MR. LOCKARD: Ms. Cooper, if we could please turn back

19   to page 62.

20   Q. So, looking again at the version of the WikiLeaks website

21   available in April of 2016, what did WikiLeaks say about a

22   service called Tails?

23   A. WikiLeaks instructs that if you are at high risk and you

24   have the capacity to do so, that you can also access the

25   submission system through Tails.

1   Q. Now, through your work, had you become familiar with the

2   Tails system?

3   A. Yes.

4   Q. And generally speaking, what is the Tails system?

5   A. Tails is a, what is referred to as a live operating system;

6   that is, it is used without being installed to your computer.

7   It is commonly placed on either a DVD or a flash drive. You

8   would put that into your computer, and your computer would boot

9   off of that device. It's a live system in that everything that

10   is happening in the operating system exists in what we refer to

11   as volatile memory; that is, nothing is saved past the power

12   cycle of the computer. And the operating system doesn't

13   actually save anything to your hard drive unless you

14   intentionally do so.

15   Q. And from the viewpoint of a digital forensics investigator,

16   what is the effect of someone using Tails on your ability to

17   recover evidence of their activities?

18   A. It makes it very, very difficult.

19   MR. LOCKARD: If we could turn to page 63.

20   Q. Mr. Berger, what's shown here?

21   A. This is the website where you would go to find information

22   about and download Tails.

23   Q. And is this version also obtained from that web archiving

24   service, the Wayback Machine?

25   A. Yes, it is.

1   Q.   And during what time period was this version of the Tails

2   website available?

3   A.   This was made available on April 22 of 2016.

4   MR. LOCKARD: And if we can turn to page 64.

5   Q.   So Tails has a description of the live operating system

6   that you just described.   What does Tails say itself about the

7   purpose and use of the Tails system?

8   A.   It talks about how it aims at preserving your privacy and

9   anonymity.   It also allows you to use the internet anonymously

10 and circumvent censorship.   It mentions how it leaves no trace

11 on the computer unless you were using it -- unless you ask it

12 to explicitly.

13 Q.   What is the relationship between Tails and the TOR network?

14 A.   So, the way Tails works --

15   MR. SCHULTE: Objection.

16   THE COURT: Overruled.

17 A.   The way Tails works is that once it's booted up and ready

18 for use, it automatically connects to the TOR network and

19 funnels anything you do in the Tails operating system over the

20 TOR network.

21   MR. LOCKARD: If we can move to slide 65.

22 Q.   What version of Tails was available in April of 2016?

23 A.   That would be version 2.2.1.

24 Q.   Now, Mr. Berger, in your review of the defendant's

25 computing equipment, did you find evidence of the Tails

M6oWsch5   Berger - Direct

1   program?

2   A. Yes.

3   MR. LOCKARD: Could we turn to slide 72, please.

4   Q. Mr. Berger, what's shown here in this slide from Government

5   Exhibit 1403-7?

6   A. This is a forensic artifact detailing details and metadata

7   about the file tails-i386-2.2.1.torrent.

8   Q. What is the significances of the dot-torrent part of that

9   file name?

10   A. So, that indicates this was a Torrent file used to obtain

11   files and share files over a Torrent network.

12   Q. And what is the Torrent network?

13   A. The Torrent network is a system designed to allow users to

14   both download files and share files they already have. When

15   you obtain a Torrent file; that is, information about the file

16   you wish to obtain, specifically what other nodes on the

17   Torrent network would have that file that you can get the

18   content from. The Torrent protocol allows you to download bits

19   and pieces of the file you want from multiple people at once.

20   Q. So, there's various pieces of information listed here about

21   that Tails-Torrent file. Were you able to conclude when this

22   file was downloaded?

23   MR. SCHULTE: Objection.

24   THE COURT: Overruled.

25   A. Yes.

1   Q. And what did you conclude?

2   A. I concluded it was downloaded on April 24, 2016, at 5:02

3   p.m. local time.

4   Q. And is that the time and date that's listed next to the

5   "last written" field?

6   A. That's correct.

7   Q. Now, there's some other date fields included here in this

8   exhibit, specifically drawing your attention to the date of May

9   10 for "last accessed" and "file created." Were you able to

10   draw any conclusions about the significance of those later

11   dates on May 10?

12   A. Yes.

13   Q. What conclusions were you able to draw?

14   A. I was able to draw the conclusion that this file had been

15   moved at that point in time from one drive to another.

16   Q. And how would that affect the "last accessed" and

17   file-created date while still remaining -- preserving the

18   last-written date?

19   A. Generally, when a file is moved between two different

20   drives or two different file systems, the last written -- or

21   also referred to as last-modified date -- is usually preserved.

22   However, because the file is now being re-created on a new file

23   system, most often the created and access times are created as

24   of new during that operation.

25   (Continued on next page)

M6oWsch5   Berger - Direct

1
1   BY MR. LOCKARD: (Continuing)

2   Q. Now looking at the file name, Tails-I 386-2.2.1, what was

3   the version of tails that was available as of April 2016?

4   A. 2.2.1.

5   Q. Now, Mr.Berger, in your review of the defendant's home

6   computing equipment, did you find a copy or a forensic artifact

7   relating to the Tails program itself?

8   A. No, I did not.

9   Q. Were you able to reach any conclusions about why you did

10 not find the Tails program?

11 A. Yes.

12   MR. SCHULTE: Objection.

13   THE COURT: Overruled.

14 Q. And what conclusions were you able to draw?

15 A. It was no longer available due to the computer drives being

16 formated at a later date.

17 Q. So you mentioned reformatting. Did your review of the

18 defendant's home computer equipment identify evidence relating

19 to data deletion and data destruction?

20 A. Yes, it did.

21 Q. If we could turn to page 82 of this slide, please? Now,

22 before we talk about that evidence, perhaps you could describe

23 for us some of the principles behind data deletion, and in

24 particular could you please describe what happens in an

25 ordinary delete command to delete a file?

1   A.   Sure.   So the way files are stored on a hard drive it can

2   be thought of as, essentially, a table of contents.   There is a

3   listing of files in the beginning of the hard drive and they

4   have locations or addresses of where the actual content for

5   those files are stored on the hard drive.   In the diagram

6   indicated here, we can see a box where it says File System.

7   That is essentially that table of contents, it is a listing of

8   files, and those files are labeled as active meaning they're

9   active, they're current, they have not been deleted.   Each of

10   those files points to a location on the actual hard drive where

11   the data for the corresponding file is stored.

12   Q.   And can you just describe how that explanation you just

13   gave of the file system is displayed in this representation

14   here on slide 82?

15   A.   Yes.   So you can see how the file system in that box has a

16   listing.   That, essentially, is the table of contents that is

17   going to list the files and it is also going to store

18   additional metadata about each files.   The cylinder on the

19   right represents the main portion of the hard drive where the

20   actual content of files is stored.

21   Q.   If we can move to slide 83, does this show what happens in

22   an ordinary deletion command?

23   A.   Correct.

24   So in an ordinary deletion command the file is marked as

25   deleted in the file system and it no longer points to the data.

1 However, the data for the underlying file in this example, file

2 3, the data is still there.

3 Q. Are you familiar with the phrase or the term "unallocated

4 space"?

5 A. Yes, I am.

6 Q. How does that term relate to the concept you just

7 described?

8 A. So if file 3 was deleted through a standard delete, the

9 address where the file 3 data is located would no longer be

10 considered allocated, it would be considered part of

11 unallocated space, that is space on the hard drive that is not

12 currently allocated to an active file and is available for

13 reuse by the file system.

14 Q. And is file data that has been deleted through an ordinary

15 delete command but remains in unallocated space, can that be

16 recovered through forensic analytical techniques?

17 A. It can be.

18 Q. Are there methods to delete files that does not leave any

19 forensic evidence behind?

20 A. Yes.

21   MR. LOCKARD: Can we turn to page 83? I'm sorry. 84.

22 Thank you.

23 Q. Mr. Berger, can you describe how a secure file deletion

24 utility would work?

25 A. In order to securely delete the file, the entire area where

1   the data file exists needs to be written over with what

2   additional data. In this slide the example is showing how the

3   content of file 3 has been overwritten with all zeros and the

4   actual entry for file 3 has been removed from the file system.

5   Q. Through your work as an FBI computer scientist, have you

6   become familiar with examples of these types of programs that

7   securely delete particular files?

8   A. Yes.

9   Q. What's an example of a utility like that?

10 A. One such program would be Eraser Portable.

11 Q. In your review of the defendant's home computer equipment,

12 did you find evidence of the use of Eraser Portable?

13 A. Yes.

14   MR. LOCKARD: Ms. Cooper, can we turn to page 88,

15 please?

16 Q. Mr. Berger, can you describe what is shown here?

17 A. So this is a screenshot from a forensic program showing the

18 file system of a thumb drive or flash drive that was recovered

19 from the defendant's apartment.

20 Q. And this is derived from Government Exhibit 1404-1?

21 A. Yes.

22 Q. And what folder are we looking at on the right-hand side?

23 A. Specifically we are looking at the Eraser

24 Portable/data/settings subfolder.

25 Q. And what type of information is stored in the settings

M6O5sch5   Berger - Direct

1   folder?

2   A.   Configuration information for the program, as well as file

3   artifacts from the use of the program.

4   Q.   Did you review the contents of these files?

5   A.   Yes, I did.

6   Q.   Let's look at slide 89. And what is shown here in this

7   slide which is derived from Government Exhibit 1404-15?

8   A.   This is what is called the schedlog.text, which is a log

9   file where Eraser Portable logs certain activities.

10   Q.   And focusing in on the entries that are highlighted in red

11   on -- or I'm sorry, on April 23rd of 2016 and April 28th of

12   2016, what type of activity is reflected there?

13   A.   On April 23rd, 2016, at 6:12 p.m., it indicates that the

14   Eraser Portable program started. On April 28, 2016, at

15   8:36 p.m., it indicates that the Eraser Portable program was

16   closed.

17   Q.   From your review of this thumb drive, were you able to

18   identify what type of activity occurred between April 23rd and

19   April 28th of 2016?

20   A.   Yes.

21   Q.   Can we turn to slide 90, please?

22   So, Mr. Berger, can you sort of describe generally what is

23   shown on this slide which is from Government Exhibit 1404-2 and

24   how were you able to use it in your forensic analysis?

25   A.   So this is, again, from a forensic program showing the

M6O5sch5   Berger - Direct

1   contents of the Eraser Portable app folder on that thumb drive

2   including recovered deleted files. Specifically, the file

3   default.ERS indicated here _efault.ERS, and you can say varying

4   in size and varying last written dates. This was a file that

5   our analysis concluded stores files that are added to Eraser

6   Portable to be queued for deletion.

7   MR. LOCKARD: If we can turn to slide 91?

8   Q. Are we now looking at the contents of one of those versions

9   of that default.ERS file?

10   A. Yes.

11   Q. And what is the date of this version of that file?

12   A. So this file was last modified on April 23rd, 2016, at

13   6:20 p.m.

14   Q. And what is reflected in the contents of that file?

15   A. There are two folders that are listed there that were

16   scheduled for deletion.

17   Q. And what is the first folder of files that was scheduled

18   for deletion on April 23rd?

19   A. The inner most sub folder is entitled Brutal Kangaroo.

20   Q. Have you become familiar with Brutal Kangaroo?

21   A. Yes, I have.

22   Q. And what is your understanding of what Brutal Kangaroo is?

23   A. It was a program the defendant worked on while he was a

24   developer at the CIA.

25   Q. And according to the file path information for Brutal

1   Kangaroo, where was the data that was scheduled to be deleted,

2   where was it stored at the time?

3   A.   It was stored in a series of subfolders that were located

4   on the D drive on the defendant's computer.

5   Q.   And can you give us just a brief overview of how the

6   defendant's home computer was set up?

7   A.   So the defendant had two different drive volumes, the C

8   drive and D drive. The C drive is where the operating system

9   was installed and that was a single hard drive. The D drive

10   was where lots of additional data was stored and that was what

11   is called a RAID volume, specifically RAID 5. That means there

12   were three hard drives connected together through a RAID

13   controller. The RAID controller combines the available space

14   on those three drives and also allows for redundancy in case

15   one of those drives fails and presents as a single volume to

16   the computer.

17   Q.   Now, does this file reflect the contents of the Brutal

18   Kangaroo folder?

19   A.   It does not.

20   Q.   Were you able to identify through your review of the

21   defendant's home computer equipment what the contents of that

22   folder were?

23   A.   I was not.

24   Q.   And why not?

25   A.   That folder was securely deleted through the use of Eraser

1   Portable.

2   Q.   And then there is also a second folder that is listed here?

3   A.   Yes.

4   Q.   And what is the name of that folder?

5   A.   Array list.

6   Q.   And do you know what the contents of that folder were?

7   A.   I do not.

8   Q.   Were you able to recover any of those files from your

9   review of the defendant's computer?

10   A.   I was not.

11   MR. LOCKARD: Can we turn to the next slide, 92?

12   Q.   So, Mr. Berger, what version of that queue file are we

13   looking at here in this slide?

14   A.   It is the version that was last modified on April 28, 2016,

15   at 8:36:36 p.m.

16   Q.   And what is listed in the queue file for Eraser Portable as

17   of April 28th of 2016?

18   A.   There are five different files named data.bkp through

19   data6.bkp.

20   Q.   Were you able to reach any conclusions about what happened

21   with these inside the Eraser Portable program?

22   A.   Yes.

23   Q.   And what were you able to conclude?

24   A.   They were added to the queue to be deleted, however the

25   programs closed before they were securely deleted.

M6O5sch5   Berger - Direct

1   Q.   And how were you able to determine that?

2   A.   Through extensive testing of the Eraser Portable program

3   and determining what types of artifacts it leaves on a drive

4   under what circumstances and essentially able to recreate the

5   timeline of deleted files we found on the thumb drive.

6   Q.   Now, from the file path information for these five .bkp

7   files, where were those files stored at the time they were in

8   this deletion queue?

9   A.   They were stored in subfolders that were located on the

10   D drive.

11   Q.   So, Mr. Berger, you said that the Eraser Portable program

12   was closed without deleting these five .bkp files?

13   A.   That's correct.

14   Q.   In your review of the defendant's home computer equipment,

15   did you identify these files or forensic artifacts of these

16   files?

17   A.   I did not.

18   Q.   And were you able to reach any conclusions about why not?

19   A.   Yes.

20   Q.   What conclusions did you reach?

21   A.   The D drive was securely wiped.

22   Q.   Now, from your review of the defendant's home computer

23   equipment, are you familiar with this naming convention of

24   data.bkp?

25   A.   I am.

1   Q. Did you find other files on the defendant's computer with

2   that naming convention?

3   A. I did.

4   Q. Did any of those files remain when you reviewed the home

5   computer equipment?

6   A. Yes.

7   Q. But not these five?

8   A. Correct.

9   Q. So, Mr. Berger, we have been talking about the secured

10 deletion of particular files or folders. Are you also familiar

11 with methods of deleting data on entire drives?

12 A. Yes.

13   MR. LOCKARD: Ms. Cooper, if we could please turn to

14 slide 82 again?

15 Q. So this is that representation of the file system and how

16 it keeps track of where data associated with particular files

17 lives?

18 A. Correct.

19 Q. Are you familiar with the concept of formatting a drive?

20 A. I am.

21   MR. LOCKARD: If we can turn to page 85?

22 Q. How does formatting a drive work?

23 A. So formatting essentially recreates the file system or what

24 we talked about earlier is the table of contents, it

25 essentially wipes out the table of contents, creates a new

M6O5sch5   Berger - Direct

1   blank slate in its place and says, OK, the drive is ready for

2   new files. It does not do anything to the underlying data of

3   those files. So as I indicated in the screenshot or the

4   diagram here, the file system is empty, it doesn't have any

5   files that it knows about or the content of the previous files

6   that existed are still present on the drive.

7   Q.   And after a format of a drive like the type you just

8   described, is that file data potentially available for recovery

9   by a forensic examiner?

10 A.   Yes.

11 Q.   Are there ways of deleting a hard drive that do not leave

12 forensic artifacts behind?

13 A.   There are.

14   MR. LOCKARD: If we can turn to page 86?

15 Q.   Can you describe how that type of disk wiping works?

16 A.   So similar as to how I mentioned earlier, a secure file

17 deletion utility would work zeroing out the content of a

18 particular file, a utility to securely wipe the entire drive

19 would overwrite all of the area on the drive. In this case it

20 is shown in the diagram as the entire area showing the file

21 system or the table of contents has been zeroed out as well as

22 all of the underlying data for the files on that drive have

23 also been zeroed out. Essentially, the program would go

24 through every available slot on that drive that could store

25 data and overwrite it with a zero or, possibly, random data.

M6O5sch5   Berger - Direct

1   Q. So, Mr. Berger, what are some of the reasons why an

2   ordinary computer user might format or reformat their hard

3   drive?

4   MR. SCHULTE: Objection.

5   THE COURT: Overruled.

6   A. Reformatting is commonly done if a user decides to possibly

7   change the operating system they are using on the computer, or

8   if it has gotten a little slow over the years and they want to

9   re-install the operating system and start fresh.

10   Q. Is a secure disk wipe necessary in order to achieve those

11   purposes?

12   A. It is not.

13   Q. Now, Mr. Berger, you have been present through the

14   testimony of some of the other witnesses at this trial; is that

15   right?

16   A. That's correct.

17   Q. And did you hear some questioning earlier today about a

18   program called Darik's Boot and Nuke?

19   A. I did.

20   Q. In your review of the defendant's home computer equipment,

21   did you find evidence relating to Darik's Boot and Nuke?

22   A. Yes, I did.

23   MR. LOCKARD: Ms. Cooper, can we please turn to page

24   95?

25   Q. So looking here at this slide which is derived from

1   Government Exhibit 1402-8, Mr. Berger, can you describe what we

2   are looking at?

3   A. So this is, again, a forensic artifact showing details of

4   metadata about a particular file. The file is entitled

5   DBAN-2.3.0 _I586.I S O.

6   Q. And were you able to reach any conclusions about when this

7   file was downloaded?

8   A. Yes.

9   Q. And what did you conclude?

10   A. It was downloaded on April 30th, 2016, at 11:28 a.m. local

11   time.

12   MR. LOCKARD: If we can turn to page 96?

13   Q. Is that the date that is highlighted here in the last

14   written field?

15   A. Correct.

16   Q. And again, I think as we saw with that Tails torrent file

17   there is later dates reflected in the last accessed and filed

18   created fields of May 5th, 2016. Were you able to reach any

19   conclusions about those later dates in those fields?

20   A. Again, that indicated that the file had been moved between

21   hard drives.

22   Q. Mr. Berger, did you do anything else with this DBAN file

23   that was found on the defendant's home computer?

24   A. I did.

25   Q. What did you do?

1   A. I copied it out of the forensic image and I created a

2   virtual machine out of it.

3   Q. And did you then operate the program?

4   A. Yes, I powered on the virtual machine.

5   MR. LOCKARD: If we can turn to page 97?

6   Q. What is shown here on page 97?

7   A. This is the main screen that appeared once the DBAN program

8   has booted up.

9   Q. In the paragraph that is highlighted in red underneath the

10   titled: "Darik's Boot and Nuke About," what is shown there?

11   A. That is information about the Boot and Nuke program and

12   essentially describes what it is and what it is capable of.

13   Q. What does it describe, if you could just read that please?

14   A. Darik's Boot and Nuke (DBAN) is a self-contained boot

15   floppy that securely wipes the hard disks of most computers.

16   DBAN will automatically and completely delete the contents of

17   any hard disk that it can detect, which makes it an appropriate

18   utility for bulk or emergency data destruction.

19   MR. LOCKARD: And if we can turn to page 98?

20   Q. Is this an additional screen that is displayed when you

21   operated the Darik's Boot and Nuke program?

22   A. Yes.

23   Q. And what does it say in the red box?

24   A. It says: Warning: This software irrecoverably destroys

25   data.

1   Q. And down below I think there is a command for listing the

2   quick commands. Did you list the quick commands?

3   A. I did.

4   MR. LOCKARD: If we can turn to page 99?

5   Q. So, generally speaking, what is described in these various

6   commands that are listed in this menu?

7   A. So these different types of wipes indicate different

8   methods of actually wiping data from a drive. I mentioned

9   before how a standard wipe would write a zero to every

10   available slot on a hard drive. Some organizations and some --

11   some organizations have developed certain types of wipes that

12   they require or recommend, for instance a three-pass wipe which

13   would be writing a single pass of zeros over the entire drive

14   three times.

15   Q. Now, in your review of the defendant's computer equipment

16   and electronic accounts, did you find additional evidence

17   relating to data destruction?

18   A. Yes.

19   MR. LOCKARD: Ms. Cooper, can we turn to page 102?

20   THE COURT: Mr. Lockard, does it make sense to stop

21   here for the day or is this a quick --

22   MR. LOCKARD: This is fine, your Honor.

23   THE COURT: So then we will break there because it is

24   2:44.

25   Ladies and gentlemen, a couple instructions, first the

1   usual ones. Don't discuss the case. Again, because it is

2   weekend you will likely be seeing family and friends, I hope,

3   but avoid the temptation to talk to them about the case in any

4   way, shape, or form. Don't discuss this with anyone. Don't

5   communicate about it any way, shape, or form. Don't do any

6   research about the case. Keep an open mind.

7   A couple things and reminders. First, just a reminder

8   that we will not be sitting next Friday but my plan is to sit

9   the four days before then and then we will break for Friday. I

10   know a couple of you had travel over the holiday weekend that

11   you had alerted us to during voir dire. We are going to

12   discuss that probably early next week, see where the case

13   stands, evaluate a variety of things. So bottom line is keep

14   Ms. Smallman apprised of any changes that you have been able to

15   make. Don't incur any greater expense without discussing it

16   with her but just keep her posted where things stand and then

17   we will try to take care of things and address it. Obviously I

18   want to balance keeping the case moving and getting all of you

19   out of here as early as we can without imposing too much on any

20   one of you if you had alerted us to prior commitments.

21   So the bottom line is more to be discussed on that

22   front next week.

23   With that, I wish you a very pleasant weekend. We

24   will pick up the same time on Monday, please be here at the

25   same time again and hopefully we will get started promptly at

1   that time.

2   Enjoy your weekends. Thank you.

3   (Continued on next page)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1   (Jury not present)

2   THE COURT: You may be seated.

3   Mr. Berger, you may step down. You are excused for

4   the weekend. Please be here Monday morning no later than 8:45

5   so that we can get started promptly when we are ready to go.

6   Have a nice weekend.

7   THE WITNESS: Thank you.

8   (Witness steps down)

9   THE COURT: Mr. Lockard, an estimate of how much

10 longer on direct?

11   MR. LOCKARD: I would give a rough estimate of about

12 another hour and a half.

13   THE COURT: And I just skimmed through the

14 demonstrative exhibit. First of all, again, as with 1703, to

15 the extent that you think any of this is admissible under 1006

16 the burden is on you to extract it and present it. Some of

17 this seems pretty cumulative of areas that were covered through

18 Mr. Leedom. Is it your intention to go through the entirety of

19 this? Am I missing something?

20   MR. LOCKARD: I think there are some discrete issues

21 in those areas that we do want to hit but I think we are going

22 to move through it pretty quickly and, of course, are conscious

23 of the cumulativeness issue.

24   THE COURT: I will take it as it comes but I would

25 urge you to pare things down, make sure you are not going over

1   ground that we have already covered.

2   Who are the next witnesses coming up the next couple

3   of days?

4   MR. LOCKARD: So after Mr. Berger concludes we expect

5   to call Jeremy Weber. After Jeremy weber we expect to call

6   Frank Stedman. And then what happens after that depends a

7   little bit on where we are in the week.

8   THE COURT: OK. Very good.

9   Mr. Schulte, I would just urge you over the weekend to

10   try to review your anticipated cross. I think some of the

11   cross that you did on Mr. Leedom, I think it got very bogged

12   down into technical details and in that sense, both the trees

13   and the forest may have been lost on the jury. I don't want

14   that to happen again but, more broadly, I don't think it is

15   fair to use the witness as a summary witness just to elicit

16   hearsay and things that they may have heard or other things in

17   the record. If there is stuff in the record that you can argue

18   from, you can argue from it. If it is the kind of thing that

19   the witness would rely on in the course of their expertise and

20   you want to ask how it impacts their analysis that is fair

21   game. But using the witness as a conduit to present hearsay to

22   the jury is not fair game.

23   The other thing is I think that just as there is case

24   law that says that you can't simply float some hypothetical

25   alternative perpetrator unless there is a nexus to the case and

1   some evidentiary basis for it. I think so, too, asking

2   questions about some theoretical possibility of some, you know,

3   remote way in which, in theory, someone could have accessed the

4   data here, unless there is some evidence to support it, I don't

5   think that that -- I think that that is sort of the same kind

6   of thing and in that sense, just asking is it theoretically

7   possible that somebody could have accessed it in this way with

8   green men from Mars, that's not fair game. I think if there is

9   evidentiary basis for it that is one thing. If it is just

10   eliciting from a witness that in a theoretical universe some

11   other way of doing this might have happened, that's not OK.

12   I don't know if the government wishes to add anything

13   on that. I assume you would agree, but.

14   MR. DENTON: Yes, your Honor. I think we were going

15   to make some observations about it this afternoon. Hopefully,

16   since Mr. Leedom is finished, this is not likely to be an issue

17   to recur.

18   THE COURT: Well, it is certainly not going to occur

19   on Mr. Leedom but I was just floating it to the extent that it

20   implicates cross for Mr. Berger.

21   Yes, Mr. Schulte?

22   MR. SCHULTE: I was just going to say I don't think it

23   is an issue for Mr. Berger. I think some of the issue was

24   simply because there were no logs available that I think some

25   of that was acceptable to raise because they don't know

1   exactly -- they didn't examine these types of things. But for

2   Berger I don't anticipate anything like that.

3   THE COURT: Good. Then it is a moot point at this

4   point.

5   We are going to reconvene in classified setting in

6   short order but before we do that, I want to see if there is

7   anything else to discuss in this setting.

8   Mr. Denton?

9   MR. DENTON: Your Honor, we would just ask that the

10   Court again make sort of appropriate findings and allocute the

11   defendant on the record about his control of his own defense.

12   THE COURT: I really don't think there is any doubt

13   about it but, in any event, no harm in belt and suspenders.

14   So, Mr. Schulte, is it correct that you continue to

15   control your defense and that you are consulting standby

16   counsel only as needed and on your own volition?

17   MR. SCHULTE: Yes. That's correct.

18   THE COURT: Anything that you wish to raise in this

19   setting, Mr. Schulte?

20   MR. SCHULTE: Yes.

21   I just want to raise that the government's letter I

22   got very late yesterday in the SCIF and the marshals were kind

23   enough to let me stay until 5:00 but I still wasn't able to, I

24   don't think, really prepare. I don't know if there is any way

25   that I could get an hour in the SCIF or something to be able to

1 specifically go through the letter and come back with things.

2 That would be helpful.

3   THE COURT: This is the letter pertaining to the

4 defense witnesses?

5   MR. SCHULTE: Yes. That's right.

6   THE COURT: Well, my thought was that we should have a

7 break before we reconvene so in that sense it would permit you

8 some time to do that. It is 2:52. I propose we reconvene at

9 3:45, which is almost an hour. Obviously you need to be

10 transported to and from the SCIF but does that work?

11   THE MARSHAL: Yes, sir.

12   THE COURT: All right. Does that work for the

13 government?

14   MR. DENTON: Yes, your Honor.

15   THE COURT: Mr. Schulte?

16   MR. SCHULTE: Yes. I just want to, on the record, the

17 marshals have been very great in all of this helping facilitate

18 this stuff, so.

19   THE COURT: Well, I very much appreciate that. I am

20 glad to hear it. Certainly they have been very accommodating

21 to my requests as well and I have told the Marshal himself that

22 I appreciate the deputies here and how good a job they've been

23 doing from my standpoint, but glad to hear it as well.

24   So if there is nothing further to discuss here, I will

25 give you as much time as we can. Let's plan to reconvene in

1   the secure setting at 3:45. Obviously, Mr. Schulte, to the

2   extent that we can go through all of the particulars in the

3   government's letter to the extent that the sooner things are

4   resolved the better we can. I guess one question is whether

5   and to what extent you are prepared to respond or would need or

6   want to respond in writing. I think there are some timing

7   issues but I think everybody has an interest in getting some

8   clarity sooner rather than later.

9   With that, we are adjourned for the day and we will

10   reconvene at 3:45 in the secure setting. I trust that you guys

11   know where it is or you will ask, otherwise trial will

12   reconvene here on Monday morning.

13   Have a pleasant weekend those of you who will not be

14   in the other courtroom. Thank you.

15   (Adjourned to June 27, 2022, at 9:00 a.m.)

16

17

18

19

20

21

22

23

24

25

13

14

15

16

17

18

19

20

21

22

23

24

25