

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,)
)
Plaintiff,)
v.) Civil Action No.:
) 2:18cv94
CISCO SYSTEMS, INC.,)
)
Defendant.)

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia
May 18, 2020

Volume 8A
Pages 1070-1156

BEFORE: THE HONORABLE HENRY C. MORGAN, JR.
United States District Judge

Appearances: (Via Zoomgov Video)

KRAMER LEVIN NAFTALIS & FRANKEL, LLP

By: PAUL JOSEPH ANDRE

Counsel for Plaintiff

DUANE MORRIS, LLP

By: LOUIS NORWOOD JAMESON

MATTHEW CHRISTOPHER GAUDET

Counsel for Defendant

I N D E X

PLAINTIFF'S WITNESSES

Page

ERIC COLE

Cross-Examination (Cont'd.) by Mr. Jameson 1077

Redirect Examination by Mr. Andre 1114

Recross-Examination by Mr. Jameson 1132

NENAD MEDVIDOVIC

Direct Examination by Mr. Andre 1143

E X H I B I T S

PLAINTIFF'S NO.

PTX-570, Page 637 1092

PTX-570, Page 638 1092

PTX-570, Page 639 1092

PTX-570, Page 640 1092

PTX-570, Page 642 1092

PTX-570, Page 594 1095

PTX-1287 1121

PTX-134 1131

P R O C E E D I N G S

(Proceedings commenced at 10:07 a.m. as follows:)

COURTROOM DEPUTY CLERK: Civil Action No. 219cv94,
Centripetal Networks, Inc. v. Cisco Systems, Inc.

For the plaintiff, Mr. Andre, Mr. Noona, are you ready
to proceed?

(No audible response.)

COURTROOM DEPUTY CLERK: For defendants, Mr. Jameson
and Mr. Carr, are you ready to proceed?

MR. JAMESON: Ready to proceed, Your Honor.

THE COURT: All right. I believe when we adjourned on
Friday there was a duel going on about packets and the newly
developed product of Cisco, and we spent a lot of time on that
and I didn't get anything out of it, so I've got a few questions
of my own for the witness.

Is Dr. Cole available?

COURTROOM DEPUTY CLERK: Yes, sir. Dr. Cole?

THE WITNESS: Good morning.

THE COURT: Good morning. There was a lot of
back-and-forth about packets and whether they went through -- or
where they went through the process of threat intelligence. I'm
not sure of what the story is here, but it seems to me that
somehow the packet went one direction and the NetFlow went

1 another direction toward, I believe it was routers to check the,
2 what threat intelligence there was in the NetFlow. It seemed as
3 if it became separated from the packets. Is that what happened,
4 Dr. Cole?

5 THE WITNESS: So NetFlow is Cisco's proprietary
6 logging, so it's a way to provide information. And NetFlow can
7 be used in two cases. So one scenario you mentioned threat
8 intelligence, so you have the StealthWatch Cloud which has
9 Cognitive Threat Analytics in it, and it can receive threat
10 analytics into the Cloud, and that can come in many different
11 ways. So we talked about Talos as one of those methods, but it
12 can also receive threat intelligence from NetFlow or any of the
13 other logging mechanisms that are out there. So that's one
14 component where the StealthWatch Cloud with Cognitive Threat
15 Analytics is getting the threat intelligence, and that can come
16 in many sources, including NetFlow. Once that threat
17 intelligence is in the Cloud, we then utilize NetFlow for a
18 separate purpose, which is as the packets go through the routers
19 and switches, those routers and switches also generate NetFlow
20 information that's sent up to StealthWatch so they can be used
21 to determine if there's threats in encrypted traffic without
22 actually decrypting it.

23 THE COURT: So there was a diagram that I remembered
24 seeing, I don't know if it was your diagram or Cisco's, that
25 showed what you're talking about. Who has that document

1 available?

2 MR. JAMESON: I believe that was Centripetal's diagram
3 that they used on direct examination.

4 MR. ANDRE: Your Honor, that was Trial Exhibit 989.

5 THE COURT: Could we put that on the screen?

6 MR. ANDRE: Yeah. It's Page 33 of that.

7 THE COURT: That's not the one that I was thinking of.
8 It was a diagram that showed NetFlow going from one direction
9 and StealthWatch sort of at the bottom right.

10 MR. ANDRE: Your Honor, that's a, a diagram that
11 defense lawyers had concocted for this litigation. We --
12 Dr. Cole has testified on Thursday that he thought that was an
13 incorrect diagram. But it's not one based on the technical
14 documents.

15 THE COURT: Well, that was the diagram I was trying to
16 remember. Could I see that one?

17 MR. ANDRE: That's from their tutorial slide. That's
18 defendant's tutorial slide.

19 MR. JAMESON: Your Honor, we're trying to pull up the
20 slide from Dr. Almeroth's tutorial.

21 THE COURT: That's the one I was thinking of.

22 Now Dr. Cole, what does that diagram represent, if
23 anything?

24 THE WITNESS: This diagram does not show the threat
25 intelligence piece. So this diagram is assuming that the

1 StealthWatch Cognitive Threat Analytics Cloud already has the
2 threat intelligence. So that piece isn't shown. But what it
3 does show is as the data comes in to the routers and the
4 switches, those routers and switches generate NetFlow data that
5 goes to StealthWatch Cloud, which utilizes Cognitive Threat
6 Analytics, and it utilizes the threat intelligence to be able to
7 determine if there's threats in encrypted traffic without
8 actually decrypting that traffic.

9 THE COURT: Okay. Well, does it show that NetFlow
10 passes through the routers and switches separately from the
11 packets? Because that seemed to be the subject of the
12 cross-examination Thursday; that somehow the threat intelligence
13 was separated from the packets. Is that your understanding,
14 that the NetFlow is somehow separated from the packets and goes
15 on a different route than the packet?

16 THE WITNESS: No. So there's two pieces. There's the
17 piece where StealthWatch with Cognitive Threat Analytics gets
18 the threat intelligence. So that's one route. And that uses
19 the same network. So there's one route where it's receiving the
20 threat intelligence so it can make decisions. And if you
21 remember from last week, that includes a domain name, that's
22 where the badguy.com came in. And then once the StealthWatch
23 Cognitive Threat Analytics has the threat intelligence, then
24 it's receiving information from the routers and switches via
25 NetFlow, and it's using that to do the analysis of the data in

1 the packets, and that NetFlow can flow over the same network,
2 it's just routed in a different manner.

3 THE COURT: Different manner than what? Than the
4 packets?

5 THE WITNESS: Than the packets.

6 THE COURT: Does that make any difference?

7 THE WITNESS: No, it doesn't.

8 THE COURT: As far as your opinion on infringement,
9 does the fact that it takes a different route affect your
10 opinion on infringement?

11 THE WITNESS: Absolutely not. So whether it takes the
12 same route or different routes, there's nothing in the claim
13 language that specifies routes and therefore the routing
14 component of how the NetFlow data arrives at StealthWatch has
15 nothing to do with my analysis. So whether it's the same route
16 or a different route, my infringement analysis would still be
17 the same.

18 THE COURT: All right. Well, that's what I wanted to
19 know.

20 All right, Mr. Jameson.

21 Somehow my screen here has four people on it.

22 MR. JAMESON: Who would you like to get rid of, Your
23 Honor? All of us?

24 MR. ANDRE: Your Honor, if you go to speaker view
25 instead of like gallery view, it will change that for you. It's

1 on the your right-hand side of your screen there.

2 THE COURT: Well, Brandan fixed it.

3 MR. ANDRE: Okay.

4 THE COURT: Now I've got Mr. Andre, and we'll go back
5 to switching between Dr. Cole and Mr. Jameson, I guess. And you
6 can resume your cross-examination, Mr. Jameson.

7 MR. JAMESON: Thank you. Your Honor.

8 CROSS-EXAMINATION (Cont'd.)

9 BY MR. JAMESON:

10 Q. And Dr. Cole, just while we're on this screen, just to make
11 clear I understand the facts, which I think I do, data coming in
12 to or packets coming in to those routers and switches is not
13 shown in this demonstrative, right?

14 A. Right. The connection between the users like User 1 at the
15 top and User 4 at the bottom is shown, but I don't see actual
16 packets, but if User 1 was going to communicate with User 4,
17 those packets would go through the router at the top and then
18 the second router to get to User 4.

19 Q. Okay. So packets would come in to the router or switch,
20 and as they're coming in a NetFlow record would be generated, is
21 that fair?

22 A. There is Encrypted Traffic Analytics on the router, so
23 there would be some analysis that would be performed. It would
24 then generate NetFlow information and send that up to
25 StealthWatch with Cognitive Threat Analytics in the Cloud.

1 Q. And the packets would continue their path to their intended
2 destination; is that right?

3 A. The packet -- so a session would be set up. So either
4 Secure Socket Layer or Transport Layer Security would set up
5 that TCP session and then those packets would go back and forth
6 between that session.

7 Q. But the packets would, the packets would go from User 1 or
8 User 2, through the router, and on to their intended
9 destination, right?

10 A. Yes. The packets as part of that connection would get
11 routed to its destination.

12 Q. Meanwhile, the NetFlow record goes up to StealthWatch,
13 right?

14 A. The NetFlow records that are generated goes up to
15 StealthWatch for analytics, correct.

16 Q. And the NetFlow record does not go to the users, right?

17 A. The NetFlow -- the packets go to the user, but the NetFlow
18 doesn't go to the user packets.

19 Q. Okay. Thank you. Let's pick up where we left off,
20 Dr. Cole.

21 THE COURT: That's what I was trying to avoid. I hope
22 we'll be a little more clear than where we were on Thursday.

23 MR. JAMESON: Well, I hope so as well. My only
24 goal -- because I know I'm not going to get him to concede
25 non-infringement, Your Honor, it's just to make sure we

1 understand his theory.

2 BY MR. JAMESON:

3 Q. So let's pull up claim 24, please.

4 On Thursday we had worked our way down to claim element F,
5 which is F, F1 and F2 on this demonstrative. And this is the
6 portion of the claim that's dealing with the first of the
7 packets based on a rule; is that right, Dr. Cole?

8 A. Yeah. There's more detail in the claim language, but
9 generally it's the part that deals with the filtering based on
10 various components, yes.

11 MR. JAMESON: Joe, could we highlight "filter" in F
12 and then the "packets" in F1 and the "determined packets" in F2?

13 BY MR. JAMESON:

14 Q. So in this portion of the claim we have five different
15 rules that are reflected in F, and based on using one of those
16 five rules, the system is filtering the packets that are
17 reflected in F1 and F2. Is that fair, Dr. Cole?

18 A. Once again, I always defer to the specific claim language,
19 but generally, yes, it's filtering on five different rules the
20 packets that are part of that session that I alluded to earlier.

21 Q. Okay. And that's actually -- I want to make sure I
22 understand your point there. What do you mean by session?

23 A. So if a user goes in and connects to a website, there is
24 going to be a TCP session -- I don't want to get too
25 technical -- but the three-way handshake, then there's going to

1 be the TLS or SSL that rides on top of that. So it's important
2 when we're looking at packets -- there's an "s" here -- we're
3 talking about all the packets as part of that session or
4 communication that's going back and forth.

5 Q. Okay. So this claim is reading on a system according to
6 your theory where the packets that are being filtered in F, F1
7 and F2 are the packets that are part of a communication session?
8 Is that what you're saying?

9 A. Yes. And that's the definition of a packet. I mean, a
10 packet is part of a communication. You could call them TCP IP
11 packets where they're part of that connection that's going back
12 and forth.

13 Q. And the communication session that you're referring to, is
14 that the same communication session that began with the creation
15 of the NetFlow record?

16 A. So I'm -- I don't understand your question. I apologize.

17 Q. Okay. Well, you previously testified that NetFlow records
18 are created and sent up to StealthWatch, right?

19 A. That is correct.

20 Q. And NetFlow records are created at the beginning of a
21 communication session; is that right?

22 A. Yes. So if you remember back at my direct when we talked
23 about the unencrypted information, we talked about the headers
24 that was going back and forth. So when a user would connect to
25 a server, that initial connection data, that unencrypted

1 information, is analyzed and utilized to then determine if there
2 is threats in the unencrypted portion without actually
3 decrypting it. So as the sessions go back and forth, as the
4 packets go back and forth as part of the session, it has
5 encrypted and unencrypted data that's being analyzed that's
6 using to determine if there's threats in the encrypted traffic
7 without actually decrypting it.

8 THE COURT: Dr. Cole, would you describe Cisco's
9 product as an attempted design around the patent?

10 THE WITNESS: No, I would not there. The infringing
11 products directly infringe on the products, so I would not
12 consider that a design-around. I would consider it an exact
13 implementation of the patent.

14 THE COURT: Well, does that mean -- could it be that
15 they were trying to design around the patent and, in your
16 judgment, they didn't succeed?

17 THE WITNESS: It's hard for me to know exactly what
18 Cisco was or was not thinking, but in my expert analysis, if
19 there was a design-around that gave them the same value and the
20 same benefits, from my experience working at similar companies,
21 you would have absolutely used that instead of infringing on the
22 patents.

23 THE COURT: Okay.

24 BY MR. JAMESON:

25 Q. All right. Dr. Cole, in the system that you are accusing,

1 where is the packet filter located?

2 A. The packet filter, that's in the StealthWatch Cloud with
3 Cognitive Threat Analytics.

4 Q. The packet filter is in the StealthWatch Cloud. Did I hear
5 that right?

6 A. Yeah. Yes. We're infringing, I believe if my memory is
7 correct, it's version 6.9.1, when the StealthWatch was -- sorry,
8 when Cognitive Threat Analytics was embedded into StealthWatch,
9 and that's the component that does the analytics and filtering.

10 Q. In order to filter packets, by definition the StealthWatch
11 Cloud must receive packets, right?

12 A. It's receiving the information from the packets via NetFlow
13 which allows it to be able to do filtering. It's receiving
14 enough information about those packets so you can still filter
15 on the packets because you're receiving that information.

16 Q. Now, Dr. Cole, I thought you just told the Court that
17 NetFlow records were sent to the StealthWatch Cloud and the
18 packets proceeded along their way to the users as part of the
19 communication session.

20 A. Based on your previous question, yes. But it's also
21 important if you remember from Thursday that the NetFlow
22 contains information about the packets and has enough
23 information that it can still perform filtering on those packets
24 based on the information it receives from NetFlow.

25 Q. So anyway, according to your theory, to meet claim elements

1 F, F1 and F2, there is actually the filtering of packets being
2 done by something in the StealthWatch appliance or the CTA
3 Cloud; is that right?

4 A. That is correct. And if we go back to my direct testimony,
5 we've showed several cases where that filtering was performed on
6 the URI information and the protocol versions, and remember
7 there were several slides that had filtering and the protocol
8 version to show that that's actually being done.

9 THE COURT: Mr. Jameson, it appears to the Court that
10 what you're trying to do is make a distinction between the
11 packet being examined and the information from the packet being
12 examined so that your expert can testify that it doesn't
13 infringe. If that's what you're trying to do, that's the way I
14 understand it.

15 MR. JAMESON: Thank you, Your Honor. And I'm going to
16 move now to the evidence that he relied on to meet claim
17 elements F through F2.

18 THE COURT: You've been doing that for 45 minutes --

19 MR. JAMESON: Your Honor, I actually --

20 THE COURT: -- yesterday and today. Longer than that.
21 About an hour. And I think I get your point. You're trying to
22 set up the field for your expert. So do we have to keep going
23 through this over and over and over again?

24 MR. JAMESON: Your Honor, he relies on three pieces of
25 evidence --

1 THE COURT: You can argue what he relies upon when it
2 becomes time for argument, and you can present evidence from
3 your expert that says it doesn't infringe because the
4 information goes to StealthWatch instead of the packet itself.
5 Seems like that's what you're trying to set up.

6 MR. JAMESON: Your Honor, actually what --

7 THE COURT: It doesn't do any good to keep asking him
8 the same question over and over again.

9 MR. JAMESON: Your Honor --

10 THE COURT: He's not going to answer it the way you
11 want him to answer it.

12 MR. JAMESON: Your Honor -- I'm sorry.

13 THE COURT: How much time -- I mean, we've been on
14 this for an hour.

15 MR. JAMESON: Your Honor, well, I think it's really
16 important for us to show the Court the evidence that he is
17 relying on to meet these claim elements, because what he has
18 done with this evidence is it's so far removed from filter
19 packet --

20 THE COURT: Don't argue your case at this point. I
21 understand what you're getting at. You're trying to set up the
22 field so that you can say you've filtered the information from
23 the packets and not the packets and therefore it doesn't
24 infringe.

25 MR. JAMESON: Your Honor, that is one, that is one

1 position we are going to establish. There is a second position
2 that's really important that we need to establish as well for
3 the purposes of this record, and I need to hit on the evidence
4 that he relied on to support his opinions.

5 THE COURT: Well, I can't imagine what other evidence
6 there is other than what you've already gotten out of him.

7 MR. JAMESON: Okay. Well, let me -- Your Honor, I
8 would just ask that you bear with me for a minute here, because
9 it's -- this is really important.

10 Can we pull up Plaintiff's 570? And can we turn to
11 Bates Page 640? And can we highlight Step 8, Filter Results?
12 Can you blow that portion up, please, Mr. Simons?

13 BY MR. JAMESON:

14 Q. Now, Dr. Cole, on Thursday you relied on this page from
15 plaintiff's 570 to show that StealthWatch filters packets,
16 right?

17 A. This was one of the components to show that the infringing
18 system can filter, and one of the things it filters on is
19 protocol version.

20 Q. Okay. Now Dr. Cole, as a matter of fact, this document has
21 nothing to do with filtering packets; is that fair?

22 A. If I remember correctly, if you can show me the title page
23 again, I believe this is the Encrypted Traffic Analytics Guide.

24 Q. Let go back to the first page for Dr. Cole.

25 It is.

1 And then let's turn to 637. And this is, this is three
2 pages before what you cited to, but this is the portion of the
3 document talking about performing a cryptographic audit. Do you
4 see that?

5 A. Yes. And in doing that, it's utilizing the information
6 that we're referring to, because ETA is embedded -- sorry,
7 Encrypted Traffic Analytics is embedded with Cognitive Threat
8 Analytics in the StealthWatch Cloud. So we're showing how it's
9 using that information and that it has that information
10 available to be able to filter on one of those five rules, which
11 in this case, being the protocol version.

12 Q. Dr. Cole, this document is literally talking about using a
13 filter function within a document as opposed to filtering
14 packets in a network, right?

15 A. In order to do that and get the information that was shown
16 in the piece of evidence that I used, the filtering would have
17 had to be performed, because that information would have had to
18 have been gathered by the system. So we're showing that the
19 information is available to that system and that information was
20 filtered from the infringing system.

21 Q. Okay. But to be clear, Dr. Cole, this is talking about
22 filtering --

23 THE COURT: Information that came from a packet.
24 That's what it's doing, isn't it? Filtering the information
25 that they got from the packets.

1 THE WITNESS: That is correct, Your Honor.

2 MR. JAMESON: Your Honor, that's what I have to
3 explore. Because this document has nothing to do with filtering
4 packets.

5 THE COURT: I didn't say filtering packets, I said
6 filtering information that was obtained from the packets.
7 That's what I said.

8 MR. JAMESON: Okay.

9 THE COURT: Isn't that what it's doing?

10 THE WITNESS: Yes, that's what it's doing, Your Honor.
11 It's showing that it is taking the information that came from
12 the patent --

13 THE COURT: Well, that's the same point you just
14 talked about before. I don't see it being a separate point.
15 Are they accused of the doctrine of equivalents as to these two
16 patents? Is that in the final pretrial order as to these two
17 patents? There was never testimony on it.

18 MR. JAMESON: That was my understanding, Your Honor.

19 THE COURT: What was your understanding?

20 MR. JAMESON: That there was no testimony on doctrine
21 of equivalents during the direct examination.

22 THE COURT: That's correct. There wasn't. So I don't
23 know whether it's part of the case or not. But it wasn't part
24 of Dr. Cole's testimony. They did bring it up on the other
25 three patents but not these two. So I don't know, is it part of

1 the case or isn't it? I mean, was that charge made?

2 MR. ANDRE: Your Honor, this is Mr. Andre for
3 Centripetal. In the case, going into it, we did have
4 allegations of doctrine of equivalents. We did not put in
5 evidence of doctrine of equivalents with Dr. Cole. We believe
6 there is literal infringement on this, and doctrine of
7 equivalents is not necessary for these patents.

8 THE COURT: Okay. All right. Well, what he's trying
9 to show is that if you get the threat intelligence and separate
10 it from the packets, send it on a different route, that that
11 means there's no infringement. That's what I understand from
12 all this questioning, and this is just the same as the other.
13 It's no different.

14 MR. ANDRE: And Your Honor, that's one of the issues
15 that I had the objection on Thursday. It's mischaracterizing
16 the patent. We're accusing the entire system, the three-part
17 system, and they're trying to parse them out as three separate
18 components. We're looking at infringement of the entire system
19 that Dr. Cole --

20 THE COURT: Well, I understand your position, and I
21 think I understand their position. And I don't know which one's
22 correct at this point. So the point is, if this is the same
23 point you made on the other part of the examination, this is
24 simply information that they obtained from the packets, and
25 apparently instead of sending the packet through the threat

1 detector, they send this information which they got from the
2 packet. Where else did it come from if not from the packet?

3 MR. JAMESON: Your Honor, I was actually --

4 THE COURT: Historic information that was --

5 MR. JAMESON: I'm sorry.

6 THE COURT: -- that was already in the system.

7 MR. JAMESON: Your Honor, I was actually trying to
8 establish a different point, but I will do this very quickly and
9 then I will move on and we'll do it with our witnesses.

10 BY MR. JAMESON:

11 Q. Dr. Cole, in connection with Plaintiff's Exhibit 570, you
12 are relying on the cryptographic audit technology within
13 StealthWatch in order to reach your opinion that claim element F
14 is met; is that fair?

15 A. I would not categorize it as that. I'm using the
16 information in this document to show that the infringing system,
17 all the components, filters on different rules, and one of those
18 things that we've seen on that previous chart was protocol
19 versions. So I'm using this as one of several pieces of
20 evidence -- we've also shown many other components in deposition
21 and source code -- this is just one additional component that
22 shows that information that comes from the packet contains the
23 protocol version, and that can be filtered on.

24 MR. JAMESON: Can we turn to 638?

25 BY MR. JAMESON:

1 Q. This shows additional steps that occur as part of a
2 cryptographic audit; is that fair?

3 A. That looks to be the case, yes.

4 MR. JAMESON: And then if we can turn to 639?

5 BY MR. JAMESON:

6 Q. This is showing more steps that can occur as part of the
7 cryptographic audit, is that fair?

8 A. That is fair, but in Step 5 it's also showing the
9 information that is available to the system.

10 MR. JAMESON: Okay. And if can we turn, Joe, to the
11 next page please, Mr. Simons?

12 BY MR. JAMESON:

13 Q. And again, this is Step 8 where you see the filter results?
14 That's what you relied on?

15 A. Yes. What we're relying on here is this is showing the
16 information that it's getting from the packets.

17 Q. Okay.

18 A. So this is showing -- even though this is an example of an
19 encryption audit, it's still showing us what information the
20 system has available to it and shows us that the protocol
21 version, which is one of the claim elements, is available so it
22 supports that the solution infringes on the patent.

23 MR. JAMESON: And then if we turn to the final page?

24 Let's go to the next page, please, Mr. Simons. Right
25 here. And can you pull up Step 11?

1 BY MR. JAMESON:

2 Q. And if you look at Step 11, it says "Once finished, you can
3 click Export and the filtered information is exported in CSV
4 format to an Excel spreadsheet." Do you see that?

5 A. I do see that language in Step 11.

6 Q. Okay. And the filtering that's being referred to here is
7 the type of filtering that you could do on an Excel spreadsheet;
8 is that fair?

9 A. I would not categorize it -- it's saying the filtered
10 information. So the information you're filtering, such as
11 protocol version and other components, that filtered information
12 from StealthWatch can be exported to CSV through an Excel
13 spreadsheet. It's not saying you pull up the spreadsheet and
14 filter within Excel.

15 MR. JAMESON: Your Honor, can we move for admission
16 the additional pages that were Plaintiff's 570, Bates ending in
17 637, 638, 639, 640, and --

18 THE COURT: Wait a minute. It was Plaintiff's
19 Exhibit 570 which has been admitted.

20 MR. JAMESON: Only one page had been admitted other
21 than the cover page, Your Honor, so I wanted to admit some
22 additional pages.

23 THE COURT: All right. Well, I would like to be able
24 to write them down. So tell me the pages you want.

25 MR. JAMESON: 637, 638.

1 THE COURT: 63 what?

2 MR. JAMESON: 638.

3 THE COURT: Okay.

4 MR. JAMESON: 639, 640 and 642.

5 THE COURT: Okay. They will be admitted.

6 (Exhibit PTX-570, Pages 637, 638, 639, 640

7 and 642 received in evidence.)

8 MR. JAMESON: Thank you, Your Honor.

9 BY MR. JAMESON:

10 Q. Now, before we leave this document I want -- just briefly I
11 want to turn to Bates 594.

12 THE COURT: Is this from the same document?

13 MR. JAMESON: Same document.

14 BY MR. JAMESON:

15 Q. I want to highlight Tech Tip. And Dr. Cole, under the
16 category Tech Tip, this states that "Cisco's cognitive
17 intelligence processes the ETA and NetFlow data in a dedicated
18 data center", and then in the last sentence it states, "Input
19 data is typically processed within two to four hours and is
20 erased after processing." Do you see that?

21 A. I do see that. Can you also blow up the two paragraphs
22 above it just so I can put the Tech Tip in context?

23 And can I take one moment just to read that?

24 Q. Sure.

25 THE WITNESS: Okay. Thank you.

1 BY MR. JAMESON:

2 Q. So the question, Dr. Cole, is it your understanding that
3 NetFlow records that are sent to StealthWatch and then
4 ultimately find their way to Cognitive Threat Analytics are
5 processed roughly every two to four hours?

6 A. Once again, just give me one second to pull the relative
7 pieces.

8 THE WITNESS: Could we go to the previous page,
9 because I think this is referring to some of the threat
10 intelligence processing, so I think we're -- we've got to be a
11 little careful we're not cherrypicking here and taking things
12 out of context.

13 Yeah, so I believe this is talking about the malware
14 detection, and it processes some of the threat analytics, and
15 once it processes it to get the threat information, then it
16 doesn't need to keep that after that processing is done.

17 THE COURT: All right. Hold on just a second, please.

18 I need to take a, just a brief recess. Five minutes.

19 Let's cut off the --

20 (Court and law clerk conferred.)

21 (Court and courtroom deputy conferred.)

22 (Pause in the record.)

23 THE COURT: Okay. Let's pick up where we left off.
24 Have you had a chance to review that, Dr. Cole?

25 (Court and law clerk conferred.)

1 THE COURT: Okay. Doctor, have you had a chance to
2 review that material?

3 THE WITNESS: Yes, I did.

4 THE COURT: You have had a chance to review it?

5 THE WITNESS: Yes, I did.

6 THE COURT: Okay. Well then let's -- can you answer
7 the question then if you can remember what it is?

8 THE WITNESS: Yeah. I think he was referencing the
9 two to four hours, and that was just talking about some of the
10 processing of the threat analytics for the malware detection.
11 In terms of analyzing threats in encrypted traffic, that doesn't
12 take two to four hours to perform.

13 BY MR. JAMESON:

14 Q. So Dr. Cole, it's your opinion that it does not take
15 anywhere from two to four hours for StealthWatch in combination
16 with Cognitive to analyze NetFlow records; is that fair?

17 A. As you saw in some cases it does, in other cases it does
18 not.

19 MR. JAMESON: Your Honor, I would ask that we move the
20 additional page from PTX-570 that ends in Bates 594 into
21 evidence.

22 THE COURT: What about 593, do you want that in too?

23 MR. JAMESON: Your Honor, since he asked to see it,
24 yes, please.

25 THE COURT: Okay. All right. They'll be admitted.

1 (Exhibit PTX-570, Page 594 received in
2 evidence.)

3 MR. JAMESON: Let's turn to the last element, Element

4 G. And can we pull claim 24 back up, Mr. Simons? Element G.

5 BY MR. JAMESON:

6 Q. And Dr. Cole, this element, it relates to routing filtered
7 packets to a proxy system; is that fair?

8 A. At a high level that is what it focuses on.

9 Q. Okay. And where is the proxy system located in the system
10 that you're accusing of infringing?

11 A. The proxy system is the null interface, which is an
12 interface on the router or the switch.

13 Q. Okay. So the filtering of packets occurred up in
14 StealthWatch and then the filtered packets are then being sent
15 to a null interface at the router or switch; is that fair?

16 A. I think you're leaving out one component. So from
17 StealthWatch for the routing, it communicates with the Identity
18 Service Engine which then communicates to the router or switch,
19 with one of the examples we've shown, quarantining, which then
20 allows it to be sent to a proxy system, which in this case is
21 the null interface.

22 Q. Okay. So the filtered packets, are they actually routed
23 first to ISE?

24 A. So once StealthWatch does the filtering, it then
25 communicates with ISE to then have to have these packets as part

1 of the session to be sent to the proxy system on the router or
2 switch.

3 Q. How do the packets that were filtered by StealthWatch, how
4 do they get to the router or the switch?

5 A. It's the packets as part of that connection, that TCP
6 connection that we talked about, Secure Socket Layer or
7 Transport Layer Security, so it's filtering on those initial
8 packets. And then the additional packets part of that
9 connection are then routed to the proxy system, in this case the
10 null interface.

11 Q. Are the packets that are being routed, are they located in
12 StealthWatch or are they located some other place?

13 A. You have the two systems that are communicating and they're
14 sending packets back and forth over the network, and information
15 of those packets is sent up via NetFlow, filtered, that
16 information is sent via Identity Service Engine to the router or
17 switch, so those additional packets that are encrypted that
18 contain threats can then be routed to the proxy.

19 Q. You recall the Court's claim construction for proxy system?

20 A. Yes, I do, and I actually utilized that, and the null
21 interface matches that claim construction.

22 Q. Okay. The Court's construction was a proxy system which
23 intervenes to prevent threats and communications between
24 devices; is that right?

25 A. That sounds to be correct. Like I said, I don't have it

1 memorized and I don't see it in front of me, but that sounds to
2 be accurate.

3 Q. Okay. And packets that are in the router or switch that
4 are being dropped, they're actually sent to the null interface,
5 right?

6 A. They're routed to the null interface. So the null
7 interface is intervening between the two entities that are
8 communicating.

9 Q. The switch actually routes them to the null interface?

10 A. The infringing switches or routers would route them to the
11 null interface, so it's meeting the claim construction of a
12 proxy.

13 Q. Okay. And when those packets arrive at the null interface,
14 it's literally a packet graveyard; is that fair?

15 A. Typically sending to the null interface is so those packets
16 can be dropped, and that's a method of intervening between the
17 two entities.

18 Q. Okay. And you're saying that the null interface is a proxy
19 system, but if you were to open up a router or a switch, you
20 actually could not touch or point to anything in a router or
21 switch that would be the null interface; is that fair?

22 A. I mean, there's components of the hardware that performs
23 it, but I don't believe the Court's claim construction says the
24 proxy has to be a physical piece of hardware.

25 Q. But I just want to be clear about that. There is not a

1 piece of hardware on a router or a switch that is the null
2 interface; is that fair?

3 A. That's not really fair, because the processor and the code
4 and the software is performing that function. So it's embedded
5 into that router or switch. So it's, it's not fair to say that
6 it doesn't consist of any of those. It's the component that
7 performs that functionality.

8 Q. Packets that are routed to the null interface, there are
9 not multiple options for the null interface to evaluate and do
10 something with them, but in every instance, the packets
11 effectively die; is that fair?

12 A. Well, the null interface is used to intervene between the
13 systems to be able to drop the packets. So its main function is
14 to drop those packets, which, once again, meets the Court's
15 claim construction for a proxy.

16 Q. It doesn't have any other function, fair?

17 A. I'm always careful with "any other". I mean, it's main
18 function is to be able to intervene between systems to be able
19 to drop packets.

20 MR. JAMESON: Okay. Well, let's turn to the '176
21 patent. And can we, Mr. Simons, pull up Joint Exhibit 3, the
22 '176 patent?

23 BY MR. JAMESON:

24 Q. Okay. Now this patent issued January 31st, 2017, right?

25 A. Yes, that looks to be the issue date.

1 Q. Okay. And with respect to this patent, you are accusing
2 StealthWatch and its integrated Cognitive Threat Analytics
3 component with any of the following: A Catalyst switch, an
4 Aggregated Services Router or an Integrated Services Router; is
5 that right?

6 A. If that's the complete list that I presented, yeah. I'm
7 going from memory, so it's always hard to remember. That sounds
8 to be correct, but I would defer back to what I presented on my
9 direct.

10 Q. You're not accusing the Identity Services Engine of
11 infringing the '176 patent, right?

12 A. That is correct. Once again, I would defer back to my
13 charts, but I believe it's the StealthWatch with the infringed
14 routers and switches.

15 MR. JAMESON: Okay. Could we turn to column 1 of this
16 patent, lines 14 to 25? Can we highlight 14 to 25? And
17 Mr. Simons, if you'll focus in on network devices? All the way
18 down to 25.

19 BY MR. JAMESON:

20 Q. Now, setting up this patent, there's a reference to
21 "Network devices located between endpoints may alter packets
22 associated with a flow, and in doing so may potentially
23 obfuscate the flow with which a particular patent [sic] is
24 associated from other network devices." Do you see that, sir?

25 A. I do see that wording.

1 Q. Can you explain to the Court generally what that's
2 referring to?

3 A. Yes. I'm pausing because I'm trying to think of a way to
4 not get too technical, because this is talking about one
5 situation with what we call Network Address Translation, where
6 IP addresses can actually be different. So when you have a
7 group of computers that are going out, sometimes the addresses
8 the source and destination address that you're actually seeing
9 in the initial packet is different than where it actually might
10 get routed to.

11 Q. And so if I understand what you're saying, packets come in
12 to a router or switch, and when they arrive at that router or
13 switch, there's this technology called Network Address
14 Translation that can sometimes cause that packet to basically,
15 it changes in a way that, when it leaves the switch, it's not
16 the same as the packet that arrived at the switch; is that
17 right?

18 A. So utilizing what we're talking about, the header
19 information of a packet that comes into the switch could be
20 different than the header information of a packet leaving the
21 switch, and that's why you want to be able to correlate those
22 two sources together.

23 MR. JAMESON: Okay. And let's pull up claim 11,
24 please, Mr. Simons, in the demonstrative.

25 BY MR. JAMESON:

1 Q. Now Dr. Cole, this is claim 11, all right?

2 A. Once again with the same caveat that this is the exact
3 wording from the patent and nothing's been altered or modified.

4 Q. Okay. And if you look at the elements B1 through B4, there
5 is a reference to a network device in each of those elements,
6 right?

7 A. That is correct. There is a network device listed in each
8 of those elements.

9 Q. And the network device is the router or switch, right?

10 A. Once again, we're not infringing individual components,
11 it's the entire system, but the component in this case that's
12 receiving and transmitting those packets is the router or
13 switch.

14 MR. JAMESON: Okay. And Mr. Simons, can we pull up
15 the demonstrative?

16 Your Honor, this is in your cross-exam notebook. It's
17 called the Ingress/Egress NetFlow slide.

18 THE COURT: Does it have a number?

19 MR. JAMESON: No, it just says Ingress/Egress NetFlow
20 slide. It's right before the trial transcript entry.

21 THE COURT: The trial transcript? Well, I don't know
22 where the trial transcript entry is.

23 MR. JAMESON: Your Honor, it's after the *Markman* order
24 and before the trial transcript.

25 THE COURT: These are trial transcript experts. Is

1 that what you're talking about?

2 MR. JAMESON: Right. And just before that --

3 THE COURT: I see it. I see it. Okay.

4 BY MR. JAMESON:

5 Q. All right. So Dr. Cole, just to try to orient us as to
6 what's happening in the accused system, we have packets that are
7 being transmitted from the first host to the accused switch or
8 router, and that's what you called on direct testimony, those
9 are the ingress packets, right?

10 A. Yes. So the left side would be what we're calling the
11 Network 1, and those packets coming in would be the ingress.

12 Q. And then the egress or the exit side are the packets that
13 are leaving the accused router or switch to go to the second
14 host or Network 2; is that right?

15 A. That is correct.

16 Q. And with respect to claim elements B2 and B4, it is the
17 ingress NetFlow record and the egress NetFlow record being
18 created that you say corresponds to those claim elements, right?

19 A. Could you just put back your mapping? I don't have your Bs
20 memorized because you used a different lettering than I was
21 using. Okay. There we go. Thank you.

22 Yeah, so B1 identifying the plurality of packets received,
23 generating the logs, identifying the packets transmitted,
24 generating logs.

25 Q. And so B2 would be the ingress NetFlow record; is that

1 fair?

2 A. That looks to be correct, yes.

3 Q. And B4 would be the egress NetFlow record; is that fair?

4 A. That would also be correct.

5 Q. Okay. And then those NetFlow records are going to be sent
6 up to StealthWatch; is that fair?

7 A. That is my understanding.

8 THE COURT: Well it doesn't show any connection
9 between those in StealthWatch on the diagram.

10 MR. JAMESON: Your Honor, you could have a, you could
11 have an arrow going from the network device straight up to
12 StealthWatch and it would just -- nobody's disputing, I think,
13 nobody's disputing that NetFlow records are sent to
14 StealthWatch.

15 THE COURT: Okay.

16 THE WITNESS: I believe in my direct we had a similar
17 diagram that actually had those arrows that actually showed the
18 connection flow.

19 MR. JAMESON: Okay. Can we go back to the claim?

20 BY MR. JAMESON:

21 Q. So we've basically addressed the elements in B1 through B4;
22 is that right?

23 A. I would say you've asked your questions on B1 through B4.
24 I believe in my direct I fully addressed the infringing
25 argument, but I addressed your questions that you had for those

1 four items.

2 Q. Okay. Now a question about the claim language: B2 and B4
3 both say "Generate a plurality of log entries." Do you see
4 that?

5 A. I do see that language.

6 Q. Okay. Is the log entry being generated, is that the
7 NetFlow record itself or is that a different log entry that's
8 being created from the NetFlow record?

9 A. NetFlow record is the plurality of log entries because
10 it's generating NetFlow for each of the packets that's being
11 received.

12 Q. Okay. So the log entry and the NetFlow record is one and
13 the same, fair?

14 A. For this claim element, the NetFlow is the plurality of log
15 entries.

16 Q. Okay. Now, during your direct and I heard you again this
17 morning, you made the comment that NetFlow is Cisco's
18 proprietary logging system. What do you mean by that?

19 A. There are many ways to get logs from a system, and it's my
20 understanding that Cisco created NetFlow as their way to be able
21 to get logging information.

22 Q. Okay. But NetFlow was invented by Cisco, what, back in
23 1996? Does that sound about right?

24 A. I would defer -- I don't have that memorized, so without
25 looking it up, but the general concept of NetFlow, it's been

1 enhanced and changed over the years, but the general concept of
2 NetFlow has been around for a period of time.

3 Q. Well, can we agree that NetFlow became an industry standard
4 in 2004?

5 MR. ANDRE: Objection, Your Honor. He's trying to get
6 invalidity back-doored in here. It has nothing to do with
7 infringement.

8 MR. JAMESON: Your Honor, I'm absolutely -- I'm trying
9 to establish the facts as to the NetFlow record that he is
10 referring to is an industry standard record. That's all I want
11 to establish. And that it's not proprietary to Cisco.

12 THE WITNESS: NetFlow is an industry standard. Once
13 again, whether it is or is not proprietary doesn't change my
14 infringement argument. I was probably referring to more that
15 they created it. But whether it is or is not proprietary has
16 nothing to do with the infringement argument.

17 BY MR. JAMESON:

18 Q. Okay. Fair enough.

19 So let's go to claim element C, which is -- there's a lot
20 of words there, but basically in claim element C we are
21 correlating the two NetFlow records that were created in B2 and
22 B4; is that right?

23 A. That is my understanding, is it's correlating based on, and
24 then it's using the language of B2 and B4, which is the reason
25 why it looks like a fairly lengthy claim.

1 Q. Okay. And the correlating that you referred to on your
2 direct examination is going to take place in the combination of
3 StealthWatch plus Cognitive Threat Analytics; is that right?

4 A. That is correct.

5 Q. And the claim specifically requires that it be the two
6 NetFlow records that you identified be correlated, fair?

7 A. The claim says that you're correlating the logs from B2 and
8 the logs from B4.

9 Q. Okay. All right.

10 MR. JAMESON: Let's pull up PTX-1065, which is an
11 exhibit that you used on direct examination.

12 BY MR. JAMESON:

13 Q. Do you recall this, Dr. Cole?

14 A. Yes, I do.

15 Q. And let's turn to Bates 005 and let's highlight the --

16 THE COURT: This is in evidence; is that right?

17 MR. JAMESON: Your Honor, this is in evidence.

18 THE COURT: Okay. And this is Bates number?

19 MR. JAMESON: 005.

20 THE COURT: Okay.

21 BY MR. JAMESON:

22 Q. Now to orient the Court, if we start, if we start -- do you
23 see the green arrow that's leading up to the StealthWatch Flow
24 Collector?

25 A. Yes, I do.

1 Q. Okay. So NetFlow records are being sent to what's called
2 the StealthWatch Flow Collector, right?

3 A. That is correct. In that box that says NetFlow Exporting
4 Infrastructure, those are the symbols for routers and switches,
5 among other things.

6 Q. Okay. So this is reflecting that the NetFlow records that
7 you've identified with respect to claim elements B2 and B4, that
8 they're getting sent up to the StealthWatch Flow Collector,
9 right?

10 A. That is correct.

11 Q. Okay. There's additional information that's being sent to
12 the StealthWatch Flow Collector and that's what's called proxy
13 data. Do you see that?

14 A. I do see that.

15 Q. And that's coming from what's referred to as Web Proxy?

16 A. That looks to be the case.

17 Q. Okay. So both types of data arrive at the Flow Collector,
18 and then if we follow the errors -- arrows, both NetFlow plus
19 proxy telemetry, they changed the word, but it's referring to
20 proxy data and NetFlow data, are sent up to cognitive analytics;
21 is that fair?

22 A. I also see that arrow.

23 Q. Okay. And cognitive analytics is then going to do analysis
24 on this data along with machine learning and threat
25 intelligence; is that fair?

1 A. It performs a series of correlation on -- and the important
2 thing for me are the ingress and egress NetFlow data. There's
3 nothing in the claim that's exclusive to just those two, so
4 there can be other data in there as long as those two NetFlow
5 records are being correlated.

6 Q. Okay. But, and just to be crystal clear about that point,
7 it's your opinion that the ingress NetFlow record and the egress
8 NetFlow record are actually correlated in Cognitive? Is that
9 fair?

10 A. In Cognitive Threat Analytics, correct.

11 Q. And just to be clear, the ingress NetFlow record and the
12 egress NetFlow record, it's your opinion this those two records
13 are being correlated with each other in Cognitive Threat
14 Analytics?

15 A. I'm trying to process -- it sounds like the same question.
16 I was trying to process if there was a difference. But yes,
17 it's -- this infringing system is taking the ingress and egress
18 logs and correlating those.

19 Q. Okay. Let's turn to Plaintiff's Exhibit 591. And again,
20 this is another exhibit that you relied on in support for
21 meeting claim element C; is that right?

22 A. That looks to be correct.

23 Q. Okay. And let's turn to Bates 522. And can we highlight
24 the paragraph under Superforest? And you relied on this
25 paragraph as support for your opinion that the ingress NetFlow

1 and the egress NetFlow are being correlated with each other in
2 Cognitive, correct?

3 A. Just for the record, I relied on a lot of pieces of
4 information, but in order to manage the time we focused on some
5 key pieces to demonstrate to the Court and this was one of the
6 many pieces of evidence that I relied on.

7 Q. Okay. Just a very simple point. Nowhere in this paragraph
8 does it state that NetFlow records are correlated with each
9 other as opposed to NetFlow telemetry and WebFlow telemetry
10 being analyzed at CTA?

11 A. Reading this entire document and all the other pieces of
12 evidence, this is one piece, in my opinion, supports that it not
13 only correlates the WebFlow and the NetFlow, but also the
14 NetFlow data is also correlated among itself.

15 Q. But just to be clear, that's not what this excerpt that you
16 relied on says, fair?

17 A. In my opinion, somebody who has read the entire document
18 would understand that it would mean WebFlow, NetFlow and NetFlow
19 among itself.

20 Q. Okay. Let's turn to PTX-1009. And this is another
21 document that you relied on, is that right, Dr. Cole, with
22 respect to claim element C?

23 A. That looks to be correct.

24 Q. Okay. And if we can go to Bates 99 -- excuse me.

25 Go to Bates 009. I'm sorry. And if we can highlight the

1 bullet under Superforest?

2 BY MR. JAMESON:

3 Q. One question, Dr. Cole: This is the identical language we
4 just looked at for the preceding exhibit as well; is that fair?

5 A. Yes, it looks to be the same line from the previous
6 document.

7 Q. Now with respect to claim element C., I don't recall you
8 providing the Court with a cite to source code to show that two
9 NetFlow records are correlated with each other in Cognitive
10 Threat Analytics; is that right?

11 A. I'm trying to parse the source code that we looked at in
12 this case, because I looked at the lot of source code. I'm
13 trying to remember which one we presented for that element. So
14 I would have to go back and check. There was a lot of
15 information from last week. I don't remember which source code
16 was which, to be honest.

17 THE COURT: Let's take our morning recess at this
18 time. We'll be in recess until 11:45.

19 (Recess taken from 11:27 a.m. to 11:48 a.m.)

20 THE COURT: All right Mr. Jameson, may proceed.

21 MR. JAMESON: There we go. Sorry, Your Honor. I was
22 on mute. Which probably was a pleasure to you. But I'm back
23 speaking now.

24 THE COURT: All right.

25 BY MR. JAMESON:

1 Q. We're going to pull up the '176 patent and turn to the last
2 elements, D through D2.

3 And to orient us all, Dr. Cole, what is happening here is
4 the correlation step has occurred in claim element C, and then
5 based on that, in D1 we are going to generate one or more rules,
6 and then the claim goes on; is that right?

7 A. Yes. The main D is the "responsive to" the correlating,
8 and then like you said, in D1 is generating a rule based on the
9 correlation, and then D2 would be provisioning a device located
10 in that first network.

11 Q. With the one or more rules?

12 A. That is correct.

13 Q. Then if we go back up to A2, you see the reference to the
14 system to, colon, and then we've been working through this.
15 Identify, generate, identify, generate, correlate, responsive,
16 and we're now going to generate a rule and we're going to
17 provision a device. The question I have is, does the system
18 generate the rule in this claim according to your understanding?

19 A. Yes. To me the system is the infringing system. It's the
20 infringing components that we've mentioned. And it absolutely
21 generates a rule and then provisions a device in the first
22 network. And one of the examples we showed was it can provision
23 a rule to the StealthWatch Management Console on the first
24 network.

25 Q. Okay. Can a human be involved in generating the rule?

1 A. The system has to have the capability, because it's a
2 system claim, it has to have the software that's able to
3 automatically generate the rule and provision a device. So that
4 can automatically be done. Whether a human is involved or not
5 doesn't alter or change the fact that that's on the system and
6 the system's capable of performing it.

7 Q. I'm not sure I completely understood your answer. If a
8 human generates a rule, is that outside the scope of this claim?

9 A. To me, there's an automatic piece. If we go back, I think
10 you're referring to some of the Court's claim construction, so
11 we have to be careful there, but the system has that capability
12 to be able to generate the rules and provision the device.

13 There could also be scenarios where there could be a human, but
14 the system has the capability, the software is built in, the
15 capability is built in to automatically do that.

16 Q. Okay. I'm going to be honest, I didn't necessarily follow
17 your answer. But let me move on.

18 What in the accused system is generating the one or more
19 rules in D1?

20 A. That is a StealthWatch Cloud with Cognitive Threat
21 Analytics, and then the device it's provisioning is the
22 StealthWatch Management Console.

23 Q. Okay. So D1, in your opinion, is satisfied by a rule that
24 is being generated by the combination of the StealthWatch
25 appliance working in combination with Cognitive Threat

1 Analytics; is that right?

2 A. The StealthWatch Cloud with Cognitive Threat Analytics.

3 Q. Okay. And then D2 is met, provisioning a device located in
4 the first network by the StealthWatch Management Console; is
5 that right?

6 A. It's the StealthWatch Cloud with Cognitive Threat Analytics
7 that can provision the device, and in this case the device
8 that's being provisioned is the StealthWatch Management Console.

9 Q. Okay. Is the rule that is being generated by -- strike
10 that. Let me start over again.

11 Is the rule being generated in D1 also known as an alert or
12 an alarm?

13 A. That could be one example of a visible component of the
14 rule. So when rules are provisioned to that device, they can
15 sometimes, in correlation with that rule, also generate an alert
16 or an alarm.

17 Q. Okay. Are there other types of rules that StealthWatch, in
18 combination with Cognitive, can generate other than alerts or
19 alarms?

20 A. There could be others, but those were the main ones we
21 focused on for my infringement analysis.

22 Q. Well, can you identify any other rules sitting here today?

23 A. I don't -- have not memorized. I'd have to defer back to
24 that section of my report.

25 Q. Okay. But you at least believe that a rule -- excuse me.

1 You at least believe that an alert or an alarm sent from
2 StealthWatch in combination with Cognitive to the StealthWatch
3 Management Center satisfies claim limitations D1 and D2; is that
4 right?

5 A. Yes, that's an example of provisioning a rule to a device
6 in the first network.

7 MR. JAMESON: Your Honor, that's all the questions I
8 have with respect to the '176 patent, so I pass the witness.

9 THE COURT: All right.

10 MR. ANDRE: May I proceed, Your Honor?

11 THE COURT: You may.

12 REDIRECT EXAMINATION

13 BY MR. ANDRE:

14 Q. Dr. Cole, I'd like to go back and want to stay on the '176
15 patent for now since we just finished that. Go back to
16 PTX-1065. Counsel showed you a figure at Page 5 of this
17 document. He showed you --

18 THE COURT: What exhibit is this?

19 MR. ANDRE: 1065, Your Honor. PTX-1065.

20 THE COURT: Okay. What page are you on?

21 MR. ANDRE: Page 5, Your Honor, of 005. Bates number.

22 THE COURT: Okay.

23 BY MR. ANDRE:

24 Q. Counsel showed you the figure at the top of the page. Do
25 you recall that?

1 A. Yes, I do.

2 Q. And he asked about the proxy data. Do you recall that?

3 A. Yes, I do.

4 Q. Let's go down to the -- blow up that figure, but let's go
5 to the text. The first five or so paragraphs.

6 Now, what does the text say about the proxy data? If you
7 look at the -- what is exactly -- they talked about the solution
8 that uses a proxy ingestion feature, a Syslog. What is Syslog
9 information?

10 A. Syslog is another form of logging. So we talked about
11 throughout this trial the different types of logs, Syslog is one
12 type. NetFlow is another type.

13 Q. And you can get the Syslog information from any of the
14 network devices just as you can get NetFlow?

15 A. That is correct.

16 Q. If you go down below, it says this Syslog information
17 contains details. Do you see that? It's the last sentence of
18 that paragraph. This system -- yeah, there we go.

19 A. Yeah. The Syslog contains details similar to what a flow
20 record contains such as Source IP, Destination IP, Source Port,
21 Destination Port, URL, Username.

22 Q. What does StealthWatch do in the next paragraph? Could you
23 describe what's being referred to there?

24 A. Yeah. So this is talking about the process. It says
25 "StealthWatch will then correlate to receive Syslog and relate

1 it to the flows collected from network devices before and after
2 the proxy, providing deeper visibility into customer web
3 traffic." So it's already performing correlation of NetFlow,
4 and then it's using this information to perform some additional
5 analysis.

6 Q. Now, if we pull out of this page and go to the very last
7 paragraph. Very last paragraph.

8 What is that referring to?

9 A. This is referring to the NetFlow data, which is in the
10 switches and routers, and that proxy data that we just referred
11 to, and it says "Customers may use either NetFlow or proxy data
12 or both." So customers can just use NetFlow by itself to do
13 that correlation. It does not need to use the proxy data.

14 Q. So when you look at this document in its entire context,
15 what does it tell you about the correlation of the '176 patent?

16 A. It shows you that correlation can be performed just of the
17 NetFlow data. So that would be the ingress and egress data that
18 we talked about. It could also perform correlation of just the
19 proxy data, or it could perform correlation of both the proxy
20 and the NetFlow.

21 Q. How does that relate to your infringement opinion as to the
22 '176 patent?

23 A. This shows that the claim language says it must be able to
24 correlate the two NetFlows. So this is confirming that it can
25 correlate NetFlow by itself which would consist of ingress and

1 egress NetFlows.

2 MR. ANDRE: Let's turn our attention to the '856
3 patent. Now if I can get Cisco's tech person to put up the
4 tutorial slide that we saw earlier today and back on Thursday as
5 well?

6 MR. JAMESON: We're working on it.

7 BY MR. ANDRE:

8 Q. Dr. Cole, have you seen any technical documents from Cisco
9 that describes their network or their system in this manner?

10 A. Not using this diagram or in the manner described here.

11 Q. And is there things in that diagram that are incorrect?

12 A. Yes, there are.

13 Q. You recall back in even the tutorial there was a statement
14 that the routers and switches cannot stop traffic, they only do
15 after-the-fact. Do you recall that?

16 A. I do remember that.

17 Q. Is that correct?

18 A. That is absolutely not correct.

19 Q. And why do you say that?

20 A. Because with the '856 particularly, if you're going in and
21 you're routing packets to the null interface, it will absolutely
22 drop packets in that communication flow and be able to stop some
23 of that communication.

24 THE COURT: What's the exhibit number of this
25 document?

1 MR. ANDRE: Your Honor, it's not an admitted exhibit.
2 This is a demonstrative created by Cisco's lawyers. It's not a
3 exhibit in this case.

4 BY MR. ANDRE:

5 Q. All right. Let's look at an actual technical document of
6 how their system actually is set up.

7 MR. ANDRE: If we can back to PTX-989, if we go to
8 Page 33 of this document?

9 BY MR. ANDRE:

10 Q. Now, first of all, let's get the components straight. In
11 the blue box in the right-hand corner it says StealthWatch. Do
12 you see that?

13 A. Yes, I do.

14 Q. Now, what is contained in StealthWatch? What is part of
15 StealthWatch in that blue box?

16 A. There's two pieces. On the left is the Management Console,
17 the Flow Collector, and in the right is the StealthWatch Cloud
18 that includes the Cognitive Threat Analytics and the Encrypted
19 Traffic Analytics.

20 Q. And do you see where there's something called Threat Grid
21 there? Is that the threat intelligence that's also part of this
22 system?

23 A. Yes, that's the threat intelligence. And you can see that
24 that's under the Cloud component. So at the bottom of that big
25 blue box that says StealthWatch there's the Cloud component and

1 an on-premise component.

2 Q. And when we're talking about the packet filtering system of
3 the '856 patent, are you considering this as a single system and
4 not separate components?

5 A. That is correct. It's the entirety of this system, the
6 routers and switches, the StealthWatch and the Identity Service
7 Engine that is the system that infringes.

8 Q. And this system does packet filtering; is that correct?

9 A. That is correct.

10 Q. Now explain how, if you had a -- if you could imagine in
11 this actual scenario, packets coming in to the Catalyst from the
12 left-hand side and leaving through the right-hand side, how
13 could packets coming in to the left-hand side be routed to the
14 proxy system before it gets to its host on the right-hand side?
15 Could you describe that scenario?

16 A. Yes. So a Secure Socket Layer connection would be set up,
17 and as some of those initial packets go through it would send up
18 to StealthWatch to get analyzed, it would determine there's
19 threats in the encrypted traffic, it would communicate with the
20 Identity Service Engine, it would then have the Catalyst send
21 the additional packets as part of that session to that proxy,
22 the null interface, and then that would contain or control the
23 damage that was being caused by that session.

24 Q. So when the Identity Services Engine -- being referred to
25 there as ISE -- when it does the Change of Authorization, which

1 is the COE, does that block or route the packets to the proxy?

2 A. Yes, that allows --

3 Q. Those rules that go down from the ISE?

4 A. Yes. Those are rules that would go down and then route
5 those additional packets to the null interface which, as we
6 discussed at length, would drop those packets or stop those
7 packets from going to the destination.

8 Q. When the packets are coming through the routers or switches
9 in this case, and you said the filtering component is up in,
10 pursuant to the claims, is up in the StealthWatch. Does part of
11 the filter have to start at the routers and switches in order to
12 get those criteria up to the StealthWatch?

13 A. Yes. It starts there because, as we discussed, the
14 switches or routers would start via ETA, determine whether it's
15 encrypted or unencrypted. So there's some of that initial
16 filtering being performed, and it continues up at StealthWatch.
17 And that, I think, is what you're referring to as it's the
18 entire system that's infringing.

19 Q. So when we talk about the packet filtering system of the
20 claims here, when they're identifying the packets with the
21 encrypted and unencrypted data, where is that being done?

22 A. Once again, it's the whole system, but the component would
23 be at the switch and the routers.

24 MR. JAMESON: Your Honor --

25 MR. ANDRE: Is there an objection?

1 MR. JAMESON: Do I have the opportunity to recross
2 this witness? He just changed his --

3 THE COURT: Yes.

4 MR. JAMESON: Thank you.

5 BY MR. ANDRE:

6 Q. So Dr. Cole, we also, we were talking about -- if we go to
7 exhibit --

8 MR. ANDRE: Your Honor, this is in your book.
9 Exhibit 1287. This is already in evidence, Your Honor.

10 BY MR. ANDRE:

11 Q. If we go to Page 28 of this document?

12 COURTROOM DEPUTY CLERK: No, it's not.

13 THE COURT: 028 Bates.

14 MR. ANDRE: 028 Bates.

15 COURTROOM DEPUTY CLERK: 1287?

16 THE COURT: Yes.

17 COURTROOM DEPUTY CLERK: It's not in evidence.

18 MR. ANDRE: I'm sorry. I thought this was already in
19 evidence. But I'd like to admit this into evidence.

20 THE COURT: All right. This is PTX-1287?

21 MR. ANDRE: Yes.

22 THE COURT: All right.

23 (Exhibit PTX-1287 received in evidence.)

24 MR. ANDRE: And I'd like to go to Page 28, Your Honor.

25 MR. JAMESON: Your Honor, I'm trying to find this

1 exhibit. Is this in your notebook, Mr. Andre?

2 MR. ANDRE: It should be in the notebook, yes. I'm
3 just going to show this diagram on the screen, Mr. Jameson, if
4 you want to look at this.

5 MR. JAMESON: Well, except I'm -- I don't know what
6 that document is and I don't think it's in my notebook. Was
7 this disclosed?

8 MR. ANDRE: I believe it was, yes.

9 MR. JAMESON: Your Honor, do you have it in your
10 notebook?

11 THE COURT: 1287?

12 MR. JAMESON: 1287. I'm just trying to locate it.

13 THE COURT: Yes, I have it.

14 MR. JAMESON: Okay.

15 MR. ANDRE: May I proceed, Your Honor?

16 MR. JAMESON: Yes. I'm good, Mr. Andre. Thanks.

17 BY MR. ANDRE:

18 Q. And Dr. Cole, this is talking about the Catalyst switching.

19 Do you see that?

20 A. Yes, I do.

21 Q. Now, at the bottom there it says "Detect and stop threat."

22 Do you see that?

23 A. Yes, I do.

24 Q. How is a Catalyst switch able to detect and stop threats

25 pursuant to the '856 patent?

1 A. It's able to detect threats by analyzing the unencrypted
2 and encrypted portions and doing that analytics in the
3 StealthWatch Cloud, and it's able to stop the threats via the
4 Identity Service Engine being able to route packets to the
5 proxy, in this case the null interface, which would drop or stop
6 the threat.

7 Q. And if you look on the right it says During. Do you see
8 that, Before, During and After? During the flow here. What's
9 that referring to?

10 A. So this is saying during the connection, so as the packets
11 are going back and forth, it's doing NetFlow-based behavior
12 analytics, it's analyzing the encrypted traffic based on the
13 unencrypted information, then it's able to do policy enforcement
14 analytics.

15 Q. Is that how it stops the threats from going into the end
16 user if it determines it's badguy.com?

17 A. That would be more on the detection, and then the actual
18 stopping the threat would be when it communicates with the
19 Identity Service Engine and then routes those packets to the
20 null interface, that would actually be stopping the threat at
21 that point.

22 Q. All right. Now last Thursday there was some --

23 MR. ANDRE: You can take that down, Geoff.

24 BY MR. ANDRE:

25 Q. Last Thursday there was some cross-examination regarding

1 your opinion of what information was disclosed to Cisco
2 during -- by Centripetal during their meetings. Do you recall
3 that?

4 A. Yes, I do.

5 Q. And you were asked if you had done any type of interview of
6 Centripetal employees. Do you recall that?

7 A. Yes, I do.

8 Q. And you said that you had reviewed the deposition
9 testimony, right?

10 A. That is correct.

11 Q. Dr. Cole, as an expert in this area, what type of
12 information would you find more useful for your analysis, that
13 type of analysis, sworn testimony under oath in a adversarial
14 proceeding, or an interview with Cisco -- I mean Centripetal
15 employees over a cup of coffee?

16 A. It would absolutely be the deposition testimony. And
17 because I looked at deposition testimony for both sides, it was
18 a much fairer analysis than just interviewing one side and
19 getting one perspective.

20 Q. Thank you. We also talked about the presentation PTX-547.

21 MR. ANDRE: And if we can pull up PTX-547? This was
22 the PowerPoint presentation. If we can go to Page 7 of this
23 document ending in Bates numbers 389?

24 BY MR. ANDRE:

25 Q. You were asked about this document when it talks about

1 Centripetal's patented filter algorithms. Cisco's counsel asked
2 you was that limited to patents not asserted here, do you recall
3 that?

4 A. I do remember that questioning.

5 Q. And if you go back to -- and you don't have to show this,
6 claim 24 of the '856, the preamble is a packet filtering system;
7 is that correct?

8 A. That is correct.

9 Q. So based on the fact they're talking about the patented
10 filtering technology at this meeting, does that inform your
11 opinion that you gave earlier on Thursday?

12 A. Yes. That further supports that the patents would fall
13 under filtering algorithms.

14 Q. And we also talked about looking at -- the value of looking
15 at contemporaneous documents. He showed you an email from
16 Jonathan Rogers that was written the very next day. Do you
17 recall that?

18 A. Yes, I do.

19 Q. We also show you --

20 MR. ANDRE: And Your Honor, I'm going to -- I don't
21 believe this was disclosed to counsel, but this is a redirect
22 question, this exhibit. This is PTX-134.

23 THE COURT: Is that out of the book? Is that what
24 you're saying?

25 MR. ANDRE: It might be in your book, Your Honor, but

1 we didn't plan on using this, but it was brought up in
2 cross-examination so it was not disclosed to opposing counsel.

3 THE COURT: PTX-134?

4 MR. ANDRE: That's correct, Your Honor.

5 MR. JAMESON: Your Honor, PTX-134 was not disclosed to
6 us over the weekend that they might be using this document in
7 redirect and it wasn't in their direct exhibits as well.

8 THE COURT: It was not disclosed to you over the
9 weekend?

10 MR. JAMESON: It was not disclosed either as part of
11 their direct examination or disclosed to us over the weekend
12 that as part of redirect they intended to go there. They
13 obviously knew they were going there, so this is the first I'm
14 seeing this document.

15 THE COURT: Well, let me look at the document.

16 COURTROOM DEPUTY CLERK: It's in your book, Judge.

17 MR. ANDRE: Your Honor, it's a long document. What we
18 were going to refer to is on Page 3. It's an email from
19 February 5th, 2016.

20 THE COURT: PTX --

21 COURTROOM DEPUTY CLERK: 134. They dropped it off
22 this morning. Should be in your direct book.

23 MR. ANDRE: Your Honor, this was --

24 THE COURT: It's in the cross-examination book.

25 COURTROOM DEPUTY CLERK: It's in that book right

1 there, Your Honor. That's your direct.

2 THE COURT: Yes, it is. All right. Let me look at
3 this.

4 Where are you focusing on this?

5 MR. ANDRE: Your Honor, it's Page 3. It's an email
6 from --

7 THE COURT: 003?

8 MR. ANDRE: Bates number 003. It's the email that's
9 from February 5th, 2016 at 4:22:49 from TKeanini.

10 THE COURT: All right. Let me look at this.

11 Well, who is the author of this?

12 MR. ANDRE: This is a Cisco engineer, Your Honor.
13 Mr. Keanini, I believe is how you pronounce his name.

14 THE COURT: And you say that they opened the door to
15 this?

16 MR. ANDRE: They did, Your Honor, when they asked
17 about the information, the contemporaneous information that
18 there was other information communicated to Mr. Rogers regarding
19 what was -- disclosing what was disclosed and not disclosed and
20 that he conveyed to Mr. Rogers. They also said that Dr. Cole
21 was not aware of the communications from Cisco's employees, and
22 this is actually in his expert report. They say that he only
23 knew how Jonathan Rogers had characterized the meeting and not
24 others.

25 THE COURT: This document was in Mr. Cole's expert

1 report?

2 MR. ANDRE: It was, Your Honor. It's on Page 28 and
3 cited in Footnote 23.

4 THE COURT: Well, there was a lot of cross-examination
5 about not... I'll allow it.

6 MR. ANDRE: Thank Your Honor.

7 BY MR. ANDRE:

8 Q. So Dr. Cole, going to PTX-134, on Page 3 you referenced
9 this in your expert report. How did this -- and in particular
10 this last paragraph, how did this inform your opinion that Cisco
11 had information about Centripetal's patented technology and how
12 it might have been used to develop their products?

13 A. So that third paragraph says "What might be worth
14 exploration is to look at these algorithms they have and how
15 general purpose they may be for data purposes. High performance
16 sets theoretical functions." So this informs me in two ways.
17 One, it shows there's absolute interest; that they wanted to
18 find out more information and more details, and two, they
19 thought they could have some value in using them in a general
20 purpose way in their systems.

21 Q. And this is the internal communication within Cisco,
22 correct?

23 A. That is correct.

24 Q. And then it talks about the next sentence, "Again, knowing
25 what patent offices will allow and not allow, I'd be surprised

1 if they're able to make claims on the algorithms itself. We
2 don't know until we study their claims." Do you see that?

3 A. Yes, I do. And this further shows me that there was
4 interest and/or intent to study the claims to find out more
5 information and more details.

6 Q. Thank you.

7 And lastly Dr. Cole, you were shown a patent by one of
8 Cisco's engineers regarding DTX-1427, and the Court ordered us
9 to provide you a copy of DTX-1427. And we did so yesterday
10 afternoon. Did you get a chance to review this patent?

11 A. Yes, I did.

12 Q. And -- well, first of all, counsel showed you a date of
13 this patent filed on August 6th, 2015. Do you see that?

14 A. Yes, I do.

15 Q. Now, in your opinion, if Cisco had developed a system to
16 handle encrypted traffic in 2015, would there be any reason why
17 they would wait over two years to implement in into their
18 products?

19 A. In my expert opinion, I would not see any reason why they
20 would wait. And also in reviewing this patent, it really
21 doesn't cover encryption/unencryption or the same technology at
22 all.

23 Q. Why do you say that?

24 A. Probably the best spot to go is if we go to claim 1, in the
25 beginning of claim 1 it actually gives a pretty good synopsis of

1 what the technology covers. And it really just talks about an
2 enhancement to data classification. But I'll wait for claim 1
3 to be pulled up.

4 Q. Column 22, line 38.

5 A. If we look at what is claimed a method --

6 Q. Go up to claim 1, please.

7 A. "A method providing improvements in efficiency of data
8 classification by transmitting datagram data rather than packet
9 data." So really it's talking about data classification and
10 just transmitting datagram information instead of packet data.
11 It's really not referring at all of analyzing
12 encrypted/unencrypted information or anything even closely
13 related to the '856 patent.

14 MR. ANDRE: Thank you. You can take that down now.

15 THE COURT: What patent was that now?

16 MR. ANDRE: This was a Cisco patent that was marked on
17 Thursday, Your Honor. It was one that they were trying -- it's
18 DTX-1427.

19 THE COURT: DTX-1427?

20 MR. ANDRE: That's correct, Your Honor.

21 MR. JAMESON: Has this been --

22 THE COURT: When was this patent granted?

23 MR. ANDRE: It was granted on May 28th, 2019.

24 THE COURT: Okay.

25 MR. JAMESON: At this point has this been admitted?

1 MR. ANDRE: I don't know if you had it admitted or
2 not. I know you showed it to the witness on Thursday.

3 MR. JAMESON: I'm sorry, Mr. Andre. I know I did not
4 move for its admission, I didn't know whether you were intending
5 to move for its admission.

6 COURTROOM DEPUTY CLERK: It's not.

7 MR. ANDRE: If you didn't move it in I won't move it
8 in either.

9 MR. JAMESON: I will be moving it in in a couple days,
10 but we'll just wait until then.

11 MR. ANDRE: All right.

12 THE COURT: So you're not moving that in?

13 MR. ANDRE: We're not moving it in, Your Honor.

14 THE COURT: All right.

15 MR. ANDRE: Your Honor, I do want to make sure we have
16 moved in PTX-134 though. I think I did, but just making sure I
17 did.

18 THE COURT: That will be admitted.

19 (Exhibit PTX-134 received in evidence.)

20 MR. ANDRE: Thank Your Honor.

21 Your Honor, I've got no further questions subject
22 to -- I assume that if they're allowed recross I can do
23 re-redirect? I don't know how many times this is going to go
24 back and forth, but I don't --

25 THE COURT: No, this is the last.

1 MR. JAMESON: I'll be very brief.

2 THE COURT: This will be the last go. I'm not, I
3 don't always allow recross, but this is a complicated case, so I
4 will.

5 MR. JAMESON: Thank you, Your Honor. May I proceed?

6 THE COURT: Yes.

7 RECROSS-EXAMINATION

8 BY MR. JAMESON:

9 Q. I want to return to your testimony, Dr. Cole, on redirect
10 with respect to the '856 patent, okay?

11 A. Okay.

12 Q. Now, when I crossed you earlier today you told me on
13 multiple occasions that the packet filter in the accused system
14 is found in StealthWatch. Do you recall that testimony?

15 A. Yes, I do. The main filtering is in StealthWatch. This
16 question was where did it begin. And it begins by analyzing the
17 encrypted and unencrypted in the router and switch, but then the
18 main filtering performs in StealthWatch.

19 Q. So just to be clear, with respect to the packet filter
20 element, it is in StealthWatch, right?

21 A. The main packet filtering where we're analyzing the
22 encrypted and unencrypted is in StealthWatch, but because ETA is
23 in the router and switch, the initial beginning of classifying
24 encrypted and unencrypted begins in the router or switch.

25 MR. JAMESON: Okay. And could we turn to PTX-547?

1 Turn to Page 7, please, which is going to be Bates 389.

2 Could we also pull up the '856 patent, which I believe
3 is Joint Exhibit 5?

4 And could you highlight the date of the '856 patent,
5 Mr. Simons? The date at the top right.

6 And could you highlight the publication date, which is
7 at 65, June 29th, 2017?

8 THE COURT: You've got publication of what?

9 MR. JAMESON: This is the publication date of the
10 patent application, Your Honor, and I wanted to ask Dr. Cole a
11 question about this.

12 MR. ANDRE: Your Honor, I object, because they're not
13 highlighting the filing date. That's when -- Centripetal
14 actually had this patent in their possession when they filed it.

15 MR. JAMESON: Your Honor, this inquiry is about
16 copying, it's not about patent infringement or invalidity. I
17 want to make a very simple point, which is --

18 BY MR. JAMESON:

19 Q. The document on the left, Plaintiff's Exhibit 547, was
20 presented to Cisco in February, 2016, right?

21 THE COURT: Presented to Cisco?

22 MR. JAMESON: A PowerPoint presentation to Cisco,
23 February, 2016.

24 BY MR. JAMESON:

25 Q. Dr. Cole, is that correct?

1 THE COURT: Who presented it?

2 MR. JAMESON: Centripetal.

3 THE COURT: All right. Can you blow that bottom left
4 up a little bit? I can't read it very well.

5 All right. This was presented to Cisco when?

6 BY MR. JAMESON:

7 Q. Dr. Cole, this was presented by Centripetal to Cisco in
8 early February of 2016; is that right?

9 A. I don't see the date in front, but I believe that is
10 correct, but...

11 Q. Okay. And then if we look to the right, which is Joint
12 Exhibit 5, the '856 patent did not issue until March 13, 2018,
13 right?

14 A. It wasn't issued until March -- sorry, it wasn't issued
15 until March 13th, 2018, but it was filed on December 23rd, 2015
16 which was before the meeting.

17 Q. Right. But it did not become publicly available until the
18 prior publication date of June 29, 2017, right?

19 A. That would be the public date, but if you remember, this
20 presentation was given under an NDA, or Non-Disclosure
21 Agreement, so it would be very common for proprietary
22 information such as a patent to be exchanged under NDA.

23 Q. And that's what I want to make sure I understand your
24 testimony on. Is it your testimony that Centripetal shared a
25 patent application that led to the '856 patent in this February,

1 2016 meeting?

2 A. It is my understanding that information about patents and
3 other data was exchanged, and it would not be uncommon under an
4 NDA to exchange information of patents that were filed but
5 haven't been issued.

6 Q. Okay. Dr. Cole, it's a very straightforward question. Do
7 you have any evidence that the application that led to the '856
8 patent was shared with Cisco at the February 4th, 2016 meeting?

9 A. I know that patent information was exchanged. I don't know
10 specifically which patents, but I know patent information
11 involved filtering algorithms which to me would include the
12 '856, was exchanged.

13 THE COURT: Well, it's got Cisco on there. They must
14 have gotten it somewhere. They said confidential and
15 proprietary. I mean, I thought -- isn't it the evidence that
16 this was shared with them in February, or we think it was?

17 MR. JAMESON: Your Honor, I'm sorry, I may have
18 confused the record here. There is absolutely no doubt that
19 Plaintiff's Exhibit 547 on the left-hand side was shared with
20 Cisco February 4th, 2016. No party is debating that issue.

21 THE COURT: All right.

22 BY MR. JAMESON:

23 Q. And Dr. Cole, that's consistent with your understanding as
24 well, right?

25 A. That is correct.

1 MR. JAMESON: Your Honor, I was just following up on
2 Mr. Andre's redirect question about what might have been shared
3 with respect to patented algorithms, and there was a reference
4 made to the '856 patent, so I was just establishing in the
5 record the actual dates and the prior publication and whether or
6 not this patent application was shared at that meeting.

7 THE COURT: How does this tell us that?

8 MR. JAMESON: Well, that's the whole point. It
9 doesn't. Your Honor, that was my point. It doesn't. And so I
10 was asking Dr. Cole whether there's any evidence that, in fact,
11 the application that led to the '856 patent was shared in that
12 meeting.

13 THE COURT: Well, I don't think that that answers the
14 question. How does this answer the question? They said -- that
15 doesn't mean that that is the only thing that was shared, it
16 just means this was shared.

17 MR. JAMESON: That's right, Your Honor. Information
18 may have been shared, but on redirect this is what they pointed
19 to as something that might have been shared, and I wanted to
20 establish with this witness that he's actually got no evidence
21 of that. That's all.

22 THE COURT: No evidence of what?

23 MR. JAMESON: No evidence that the application that
24 led to the '856 patent was shared with Cisco at this
25 February 4th, 2016 meeting.

1 THE COURT: All right.

2 BY MR. JAMESON:

3 Q. Dr. Cole, you do not have any evidence on that point,
4 correct?

5 A. The evidence I have is that Centripetal had this patent
6 December, 2015, they signed an NDA, and they discussed
7 proprietary information, including patents, at the 2016 meeting.

8 Q. Let's wrap this up by turning briefly to PTX-134, which is
9 the emails that you discussed a few minutes ago. Do you recall
10 that?

11 A. Yes, I do.

12 MR. JAMESON: Let's turn to what would be Bates 003.
13 And if we could look at the second paragraph and highlight that?
14 And can you move that down so we can see who is saying this?

15 BY MR. JAMESON:

16 Q. And just to be clear, Dr. Cole, this is internal
17 correspondence at Cisco, correct?

18 A. That is correct.

19 Q. And Mr. Keanini says "I'm not sure the market will see this
20 as high value, as the systems they have in place doing this type
21 of work today seem to be working just fine." Do you see that
22 statement?

23 A. Yes, he does say that, but then as we showed in the
24 following paragraph, he still indicates that further research
25 would potentially be beneficial.

1 Q. And then if we continue with the email chain going back to
2 the previous page, but we are fast-forwarding in time. Take a
3 look at an email from Michal Pechouc. He's responding to
4 Mr. Keanini, right?

5 Are you there, Dr. Cole?

6 A. Yes. This looks to be the case. He's replying to TK.

7 Q. And he states in the first paragraph, highlighting
8 beginning with "There," the next two sentences? He states
9 "There is general agreement that the value they're bringing to
10 the table is scalability and fusing the intelligence and doing
11 signature-based detection. The rest is not that important, I
12 would say." Do you see that statement?

13 A. I do see that.

14 Q. That's a reference to Centripetal's pitch that they could
15 literally analyze every packet traversing a network using
16 5 million rules, and they believed that was the innovation they
17 could bring to the table; is that fair?

18 A. I would not agree with that. When you're looking at fusing
19 the intelligence, that could be correlation, that could be
20 examining threats in encrypted traffic flows without decrypting
21 it, and that's a fairly broad area. So I would see that in my
22 expert opinion, when they say scalability fusing the
23 intelligence, that would also cover the technology in the '856
24 and '176 patents.

25 MR. JAMESON: Let's go up to next email, Mr. Simons.

1 BY MR. JAMESON:

2 Q. And again, continued email correspondence among the team
3 that received the February 4, 2016 presentation.

4 Can we highlight the bottom?

5 And this is an email from Mr. McDonough at Cisco, and he
6 states "TK, Michal thanks you for your feedback. After the
7 call, my conclusion was that Centripetal networks is an IPS on
8 steroids, meaning they have a larger signature base than we did
9 at SourceFire, approximately 10,000 rules" --

10 Then go to the next page.

11 -- "versus their approximately 5 million rules in
12 approximately 10 microseconds based upon multiple input sources
13 of threat intel." Do you see that?

14 A. Yes. But I think it's important to point out that this
15 individual came from SourceFire, so he's going to be doing his
16 analysis based on SourceFire. So each one of these folks have
17 different perspectives. But I think it's important to point out
18 the last sentence that he's happy to continue investigating,
19 showing that there's still interest in the technology.

20 Q. Okay. So let's go up to the next email. And from
21 Mr. Parthasarathi, he responds to the email chain and says
22 "Centripetal Networks is planning to launch a Series B
23 investment round. Please let me know if you found the
24 technology interesting enough for us to further explore." Do
25 you see that?

1 A. I do, and I believe the reply at the very top is that he
2 indicated that Michal wanted to do a deep dive.

3 Q. We're not there yet, Dr. Cole. Let's focus on this right
4 here.

5 Do you see what I'm referring to?

6 A. Yes, I do.

7 Q. Okay. So the question on the table for Cisco is whether or
8 not they might be interested in investing in Centripetal, right?

9 A. That's one way to look at it, that they are looking at it
10 for investment or potentially licensing or potentially
11 purchasing the technology. There can be many different angles
12 that a large company like Cisco would be interested in exploring
13 with an innovative company like Centripetal.

14 Q. Then we go up to the next email. This one is from
15 Mr. Subramanian. And he states "Hey, I thought the feedback was
16 not that compelling based on email from TK and Michal. Did I
17 get this wrong, question mark." Do you see that?

18 A. Yes, I do.

19 Q. Okay. And the final email comes back from
20 Mr. Parthasarathi, "It wasn't explicit. Michal indicated the
21 need for a deeper dive. We have not received the feedback from
22 Bret. Hopefully he will let us know." Do you see that?

23 A. Yes, I do.

24 Q. And here is what we know based on all of the documents in
25 evidence that you reviewed in this case: That four days later,

1 Cisco reached out to Centripetal and told them they were not
2 interested in investing in Centripetal. Do you recall that?

3 MR. ANDRE: Objection, Your Honor. Not in evidence,
4 he's testifying.

5 MR. JAMESON: I'm actually -- he's reviewed all the
6 documents in the case. I'm asking whether he recalls that.

7 THE COURT: I think it's a proper question. If he
8 recalls it or not. I don't know what his answer is.

9 THE WITNESS: So I can answer, Your Honor?

10 THE COURT: Yes.

11 A. Okay. I do know at some point Cisco decided not to pursue
12 the engagement. I don't remember the exact dates.

13 MR. JAMESON: Thank you.

14 No further questions, Your Honor.

15 THE COURT: All right. So much for Dr. Cole's
16 testimony. Is there any possibility that he may be recalled as
17 a witness?

18 MR. ANDRE: No, Your Honor. Dr. Cole is released from
19 this case.

20 THE COURT: And I assume that defense agrees to that?

21 MR. JAMESON: Absolutely, Your Honor.

22 THE COURT: All right. Dr. Cole, you are released as
23 a witness, and if you wish, you can participate in the case by
24 listening in, but you are not permitted to discuss your
25 testimony with any other witness in the case until the case is

1 concluded. So you may be excused. And as I say, you can listen
2 in if you want.

3 THE WITNESS: Thank you, Your Honor.

4 THE COURT: You may have something else you'd rather
5 do.

6 THE WITNESS: Thank you.

7 THE COURT: All right.

8 MR. ANDRE: So Your Honor, that is the last
9 infringement witness we have. We have some witnesses regarding
10 willful infringement, but we're going to begin for the most part
11 the remedies aspect of the case now with both, for past damages
12 and looking forward and with that, we're going to call, recall
13 to the stand Dr. Nenad Medvidovic. He was the person that we
14 had originally proposed to give the tutorial in this portion of
15 his testimony as well regarding the benefits of the patented
16 technology. So we've done the tutorial part, now we're just
17 going to do a very short benefits of the technology here.

18 THE COURT: Well, what does very short mean?

19 MR. ANDRE: I think we'll be done by lunch.

20 THE COURT: All right.

21 MR. ANDRE: We hope. You know, we'll see if Dr.
22 Medvidovic can gets it done in time.

23 THE COURT: Well, usually five or 10 minutes usually
24 lasts about half an hour.

25 MR. ANDRE: Well, we are hoping. I'll let Lori swear

1 him in.

2 THE COURT: All right.

3 NENAD MEDVIDOVIC, having been duly sworn, was examined
4 and testified as follows:

5 MR. GAUDET: Your Honor, this is Matt Gaudet for
6 Cisco. We've switched up the faces and voices on our end. I'll
7 be handling the objections and the cross-examination of Dr.
8 Medvidovic.

9 THE COURT: All right.

10 MR. ANDRE: May I proceed, Your Honor?

11 THE COURT: You may.

12 DIRECT EXAMINATION

13 BY MR. JAMESON:

14 Q. Dr. Medvidovic, let's start off by remind in the Court of
15 your qualifications in this case. Would you talk about your
16 education first?

17 A. Sure. I received my Bachelor of science in computer
18 science and engineering from Arizona State University, and my
19 Master's and Ph.Ds from the University of California at Irvine.
20 Both of those degrees were in information and computer science.

21 Q. And where do you currently work and how long have you been
22 there?

23 A. I have been at the University of Southern California for
24 slightly over 21 years at this point in time.

25 Q. And what's your title there?

1 A. I am a full professor of computer science with tenure.

2 MR. ANDRE: Your Honor, we've already gone through his
3 background before, I'd just like to go ahead and tender him as
4 an expert in computer science and computer architecture, if
5 there's no objection. I don't know if Your Honor wants me to --
6 I can go deeper into his background if you'd like to hear some
7 more.

8 THE COURT: Is there any voir dire on his expertise?

9 THE DEFENDANT: No, Your Honor. And I don't know if
10 they intend for Dr. Medvidovic to offer a copying opinion along
11 the lines of what Dr. Cole did. If he does, we may seek voir
12 dire at that point. But in terms of the scope that he was just
13 proffered, and if it's about the benefits of the patent, we
14 wouldn't have anything. So nothing now, and if we hear
15 something about copying we may revisit.

16 THE COURT: All right. You may proceed.

17 MR. ANDRE: Thank Your Honor.

18 BY MR. ANDRE:

19 Q. So Dr. Medvidovic, you started off this case with the
20 tutorial. What was your additional assignment with respect to
21 this case?

22 A. I was asked to opine on a couple of additional things. The
23 first one was the importance of the technology described in the
24 asserted patents on cybersecurity, or to cybersecurity, and the
25 other one was -- or the second one was determining the

1 importance of the technology described in the asserted patents
2 to the products accused in this case.

3 Q. And we've already heard a lot of this, but let's start with
4 the groundwork of where the threat landscape was, what it looked
5 like in the 2010 time period.

6 A. Sure. So this is a diagram that came out of one of the
7 Cisco documents, and it just kind of at a very high level,
8 describes how the threat landscape has --

9 THE COURT: Everybody keeps saying "at a very high
10 level." What's the difference between a high-level and a
11 low-level?

12 THE WITNESS: Your Honor, the reason why this is at a
13 high level is, for example, if you look at the year 2000, it
14 just says it's worms. Worms are basically self replicating
15 pieces of malware. There is a lot of stuff that has gone into
16 how those things are fought by the computer security industry,
17 and of course probably a lot of work by what we call the bad
18 guys into how to make the worms ever smarter, for example. So a
19 lot of stuff is sort of swept under the rug just by popping up
20 that one bar and saying worms. That's what I mean by
21 high-level. So this just kind of gives a very general overview
22 of the trend in the industry without describing really any of
23 the lower-level details. So for example, in roughly --

24 THE COURT: Seems like to me you've got high and low
25 backwards, but...

1 THE WITNESS: Fair enough.

2 A. It associates roughly with the year 2005, the emergence of
3 spyware, so that somebody is able to, without your knowledge,
4 get into your computer and figure out what's going on there.

5 Same thing with rootkits, which are ways for, again, a bad
6 guy to get a hold of your computer and be able to control it
7 without you necessarily realizing that. And at about the year
8 2010 they associate that time frame with Advanced Persistent
9 Threats and cyber warfare. And that's essentially things like
10 somebody consistently siphoning off information from you,
11 somebody being able to do things like Denial of Service attacks,
12 for example. So kind of more sophisticated types of things.

13 And then eventually the prediction at that time when this
14 document was put together was that what we're going to be facing
15 going forward and certainly some of that has come true, is that
16 we're going to have these what they call increased attack
17 surfaces, meaning that we're going to be exposed in a lot more
18 ways, and for that, the suggestion is that what is needed to
19 fight that would be this whole thing dealing with intelligence
20 and analytics that would be brought to bear on those kinds of
21 attacks.

22 THE COURT: All right.

23 BY MR. ANDRE:

24 Q. So Dr. Medvidovic, is high-level sort a catch phrase that
25 you hear from computer science a lot of times because they love

1 getting down in the code and the weeds at a low level?

2 A. So I'm a software engineer and researcher by training, and
3 one of the basic principles of software engineering is
4 abstraction. It's kind of hiding the details and elevating the
5 discourse to a point where people can have a, hopefully,
6 meaningful conversation about it. So we try to distinguish the
7 high-level from the low-level, which to us is the weeds. Source
8 code and things of that nature that Your Honor saw in the
9 infringement testimony.

10 BY MR. ANDRE:

11 Q. That's not to be confused with obfuscation, right?

12 A. No. In fact, abstraction is --

13 THE COURT: I notice we even found that in one of the
14 claims, didn't we? Obfuscation in there?

15 THE WITNESS: Obfuscation is a common technique used
16 by these proverbial bad guys to disguise themselves.

17 THE COURT: That's not the only person who uses it.

18 THE WITNESS: So I can only talk about in the context
19 of the technology here. I think Your Honor was using that term
20 a couple of times so far in a slightly different context and I
21 will have no comment on that.

22 THE COURT: All right.

23 BY MR. ANDRE:

24 Q. All right. So let's go talk about the Centripetal patents
25 in this case and how they attempted to -- and the importance

1 they have on the cybersecurity field.

2 If you could just once again go through the patents and
3 describe this very generally?

4 A. Sure. So we have seen a lot of testimony on all five of
5 these patents, and there were these terms that we associated
6 with the different patents. So for example the '193 was the
7 forward or drop patent; the '806 was the rule swap patent; the
8 '205 was the dynamic security policy patent; the '856 was the
9 encrypted traffic patent, and the '176 was the correlation
10 patent.

11 THE COURT: Well, it seems to me if you add all the
12 patents up, what they attempt to do is adopt new rules before a
13 decision is made on whether or not to adopt -- or they adopt
14 their rules in advance of deciding whether the package moves
15 forward instead of waiting until the packet reaches its
16 destination, and then taking what historically has gone wrong
17 and building that into the rules. So they try to keep the rules
18 up-to-date and apply them before the decision is made instead of
19 after the decision is made, or until after the packet reaches
20 its destination. Is that a summary of what they're trying to do
21 here?

22 THE WITNESS: That is a rather accurate way of --

23 THE COURT: A high-level summary?

24 THE WITNESS: Your Honor, I think you're catching on
25 to the gist here, yes. That is a pretty accurate way of

1 describing what the motivation and the idea behind these patents
2 is. And the reason why there are five of them is they really
3 teach different pieces of this puzzle, so that, for example,
4 '193 just teaches about whether you should allow a packet to get
5 forwarded or to be dropped. On the other hand, '856, for
6 example, says, well, you can do some of those things also with
7 encrypted traffic. '176 builds on top of that and says, well,
8 given how computer networks actually work, you can program, log
9 these various things, you can do these sophisticated
10 correlations, and then that will allow you to make these
11 determinations so that, in fact, the things that you do not want
12 to see happen, which is what Your Honor just said a second ago,
13 which is have that packet, if it's not supposed to reach
14 somewhere, have it actually reach there. That's the undesirable
15 effect, you would like to actually be able to stop that from
16 happening. So these five patents essentially come together in a
17 sort of holistic way and enable various aspects of this problem
18 to be solved.

19 THE COURT: Well, the problem of course is magnified
20 by encryption. So what these patents attempt to do -- and I'm
21 using the word "attempt", because the Court's got to decide not
22 only infringement but validity, so everything is up in the air
23 at this point -- but what they attempt to do is bring new forms
24 of threat intelligence into the decision-making process in
25 advance rather than in retrospect. In other words, by the time

N. Medvidovic - Direct - Andre

1150

1 you -- what's the word -- unencrypt or de-encrypt, it's too
2 late. So you've got to figure out what's malware or -- I'm not
3 good on all this, but you've got to decide it before you decide
4 whether to drop it. You can't wait until after it reaches the
5 destination, because once it reaches the destination the damage
6 is done, and the only thing you can use that information for is
7 to say, well, we won't let this same thing happen again. But
8 what this technology is trying to do is prevent it from
9 happening in the first place, even to encrypted traffic, right?

10 THE WITNESS: That is exactly correct, Your Honor.
11 And what you're getting at is -- by the way, your terminology in
12 what you describe are, in fact, spot-on.

13 I will introduce two other terms, because what you've
14 described is the difference between proactive techniques, which
15 are ones that try to determine what happens before it has some
16 sort of a negative effect, and reactive techniques, which are
17 traditionally have been able to act on things only after some
18 damage has been done. And so in a way, you can think of it,
19 right now we're dealing with a pandemic where humanity is
20 reacting. People got infected, there were effects, those
21 effects were being observed, and now we're kind of retroactively
22 trying to figure out how to address that. So that whole
23 dichotomy between proactive and reactive turns out to be very
24 important in the computer security industry.

25 THE COURT: All right.

1 BY MR. ANDRE:

2 Q. And I noticed also with respect to the '193 patent, Dr.
3 Mitzenmacher talked about a concept of exfiltration. Now, could
4 you explain how these patents relate to the exfiltration as
5 well, of data once you do get infected, keeping it from going
6 out?

7 MR. GAUDET: Your Honor, I would object that that
8 sounded a little leading to me at the end there.

9 MR. ANDRE: I'll withdraw the question.

10 BY MR. ANDRE:

11 Q. Dr. Medvidovic, could you talk about exfiltration and how
12 these patents relate to it?

13 A. Sure. So there are no sure bets in computer security, just
14 like there are probably no sure bets in many different walks of
15 life. So the expectation is that occasionally things will, in
16 fact, get through that may in some way harm your system. And
17 one of the things that can happen in those situations -- and
18 that was also something that was recognized on that previous
19 slide that we put up of Cisco -- one of the things that can
20 happen is by having somebody, for example, do a rootkit type of
21 thing, what they can do is they can start siphoning off your
22 proprietary information and sending it to a place where it's not
23 supposed to go because you don't want it there, and whoever is
24 potentially going to be able to see it there is not actually
25 authorized to see it. So what these patents actually talk about

1 also is if that were to happen, in other words, given that we
2 cannot assume that there are sure bets in computer security, if
3 things were to get there, can we remedy that anyway? And this
4 idea of controlling the data going the other way, this
5 exfiltration, addressing the exfiltration, is a very important
6 aspect of these patents.

7 THE COURT: Well, I mean, exfiltration could mean
8 learning my credit card number. It could also operate on a
9 foreign power learning communications relating to find a vaccine
10 for the virus.

11 THE WITNESS: Absolutely. And that's one of the more
12 insidious aspects of cyber warfare, is that the players are no
13 longer, as President Trump said in one of his debates three or
14 four years ago, they're no longer the 350-pound guy sitting in
15 his basement. The bad guys in that case are actually state
16 actors: People who are highly trained who know what they're
17 doing, who are trying to exploit this for much more serious and
18 nefarious kinds of purposes.

19 BY MR. ANDRE:

20 Q. And so these patents also, they stop traffic, bad traffic
21 coming in, also traffic going out to the bad guys. They stop
22 traffic both ways?

23 MR. GAUDET: I object. That was leading.

24 THE COURT: Okay. Well, I don't think that's worthy
25 of an objection.

1 MR. GAUDET: Understood. Thank you.

2 THE COURT: I overrule the objection.

3 I mean, this exfiltration could also, in addition to
4 gaining information that's supposed to be secret because its
5 encrypted, it could be also remove malware which might infect
6 the recipient's ability to utilize the information being sent to
7 them. In other words, it may be a virus that's encrypted. A
8 secret virus. Can it remove a secret virus from the packet so
9 that virus won't infect the recipient in addition to --

10 THE WITNESS: Your Honor, typically the short answer
11 is yes. The slightly more detailed answer to just clarify
12 there, a virus will typically not be embodied in a single
13 packet. You would need multiple packets to kind of assemble the
14 virus wherever you send it. And what this would do is it would
15 recognize through these various techniques that we talked about,
16 for example, identifying encrypted traffic, looking at the logs
17 to do the correlations, what it would do is it would figure out
18 that that are going to be some of these packets, sequences of
19 these packets, that should not be allowed to go through, for
20 example. Or if somehow they did get through, then they should
21 not be allowed to somehow do their damage by sending sensitive
22 information going the opposite way.

23 THE COURT: What do you mean "sending information
24 going the opposite way"? I understand that somehow based on the
25 volume and a combination of the volume, source and other

1 characteristics of the way the package is transmitted you
2 conclude that there's malware. You would just drop the packet.
3 Packets, plural.

4 THE WITNESS: That is correct, Your Honor.

5 THE COURT: And we've talked about what happens, a
6 little bit about what happens to the packet after they're
7 dropped. I mean, after they're dropped they could be
8 unencrypted or de-encrypted, I don't know which is the right
9 word, and we could find out what the malware was. But that
10 would take time.

11 THE WITNESS: That is all correct, Your Honor. The
12 reason why these patents are, in a sense, using an abundance of
13 caution, is because it's been recognized now for a really long
14 time that hackers tend to stay a step ahead of security
15 solutions. So it is not wise to assume, even though you might
16 have world-class technology like nothing that has ever been
17 built before, it is still considered unwise to assume that
18 nothing will ever get through. So this is the whole idea of
19 defense in depth. If something were to -- so of course the
20 scenario that you described, if these packets go through, you
21 catch them using the various techniques we've talked about as
22 part of this case, and you drop them, for example, using that
23 null interface proxy that Dr. Cole talked about. That's one
24 scenario.

25 Another scenario is let's consider it a worst-case

1 scenario for any security technology, is somehow these packets
2 get to the end device, somehow they get on your computer. What
3 can be done then to minimize the damage? So how can you contain
4 that damage? In other words, what is that last line of defense
5 that you have on your computer that can still sort of make it
6 possible for you to sleep at night; that even if you have this
7 worst-case scenario and some new hacker came up with something
8 that has never been seen before, what can you do to mitigate any
9 possible damage that that new sort of super-futuristic piece of
10 malware is going to try to do? You would like to deal with that
11 as well. So deal with things you haven't even thought of today,
12 still be able to address those.

13 THE COURT: Well, if the malware reached the recipient
14 it's too late, isn't it? I mean, all this technology is
15 designed to keep it from getting there. If it gets there, the
16 technology hasn't worked, has it?

17 THE WITNESS: Your Honor, it's too late for some types
18 of malware. Although they will get caught at the very last
19 step, very often most often by typical anti-malware software
20 that you might have installed on your computer. Most
21 organizations do provide this for the devices. So my university
22 does, and it kind of runs on my computer in the background all
23 the time, trying to catch these things based on techniques that
24 are pretty well-known, but really are kind of outside the scope
25 of this case.

1 The more intelligent, newer generation bad guys, if
2 you will, they will not just do sort of the high school kid from
3 Bulgaria trick of getting on your computer and just kind of
4 infecting your files just for kicks. What they will try to do
5 is they will try to figure out, first, how they can disguise
6 themselves so you don't notice they're there, and second, they
7 will slowly start siphoning off this information, because
8 information is power. And the example that you mentioned, for
9 example, your credit card number. We enter our credit card
10 numbers into our computers using our keyboards all the time. If
11 there is a silent piece of malware sitting somewhere undetected
12 on your computer, what can you do to prevent that credit card
13 number from getting to an undesirable destination. And that's
14 the idea of exfiltration being dealt with by these patents.

15 THE COURT: Okay.

16 MR. ANDRE: And Your Honor, I realize we are past the
17 lunch hour here. Would you like to take the lunch break now?

18 THE COURT: Yes. Probably would be a good time to do
19 that. Let's take a recess until 10 minutes after 2.

20 (Recess taken at 1:07 p.m.)
21
22
23
24
25

CERTIFICATION

I certify that the foregoing is a true, complete and correct transcript of Volume 8A of the proceedings held in the above-entitled matter.

Paul L. McManus,
OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US,
email=pmcmanusocer@verizon.net
Date: 2020.08.10 13:39:50 -04'00'

Paul L. McManus, RMR, FCRR

Date

Paul L. McManus, RMR, FCRR Official Court Reporter

Patent Owner, Centripetal Networks, Inc. - Ex. 2017, p. 88