

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT
Petitioner,

v.

CENTRIPETAL Patent Owner

IPR2023-00446
Patent 10,567,343

Held: May 6, 2024

BEFORE: KEVIN F. TURNER, AARON W. MOORE, and
STEVEN M. AMUNDSON, Administrative Patent Judges.

IPR2023-00446
Patent 10,567,343

APPEARANCES:

ON BEHALF OF THE PETITIONER:

GERARD DONOVAN, ESQUIRE
Reed Smith, LLP
1301 K Street, NW
Suite 1000-East Tower
Washington, DC 200015
gdonovan@reedsmith.com
(202) 414-9299

ON BEHALF OF THE PATENT OWNER:

JEFFREY PRICE, ESQUIRE
Kramer Levin
1177 Ave of the Americas
New York, NY 10036
jprice@kramerlevin.com
(212) 715-8302

JAMES HANNAH, ESQUIRE
jhannah@kramerlevin.com
(650) 752-1812

The above-entitled matter came on for hearing on
May 6, 2024, commencing at 1:00 p.m., via video teleconference.

P R O C E E D I N G S

- - - - -

JUDGE TURNER: Good morning or good afternoon. This is an oral hearing in IPR2023-00446 involving a U.S. Patent 10,567,343. I am Judge Turner, and I'm joined by Judges Moore and Amundson. For the benefit of the Judges and for the benefit of counsel, we have, and as well as a court reporter, we ask that you please identify yourself when you begin your argument and speak clearly into your microphone. Please do not speak when others such as the Judges are speaking. We have the entire record, including demonstratives. When referring to demonstratives, papers, or exhibits, please do so clearly and explicitly by slide or paper number. Please also pause for a second after identifying it to provide us the time to find it. This helps with the preparation of an accurate transcript of the hearing.

Please bear in mind that the purpose of oral hearing is to present your case based on the arguments and evidence of record. You may not introduce new evidence or arguments during your oral argument. I note that there do not appear to be any objections to the demonstratives from either side. Please note that we do not permit standing objections to be raised during opposing counsel's during their arguments. If an advocate believes that new evidence or arguments are being raised, he or she may make that known to the panel during their principal argument or rebuttal arguments. Each party will have 45 minutes of total argument time. Petitioner and Patent Owner may reserve time for rebuttal. Petitioner will go first and present a case. Thereafter, Patent Owner will argue its opposition

1 to Petitioner's case, and if there's any rebuttal from Petitioner, we will hear it
2 after Patent Owner's opposition.

3 Finally, we will hear Patent Owners sur-rebuttal if requested. I
4 will endeavor to provide each party with a five minute warning during
5 opening arguments and a two minute warning during rebuttal or sur-rebuttal.
6 Once I've given you that indication, please finish up your argument or let the
7 panel know you wish to extend your arguments into prearranged rebuttal or
8 sur-rebuttal time is available. Please also note that arguments raised during
9 rebuttal or sur-rebuttal must be in response to arguments raised by the
10 opposing party. Neither period should be used to initiate your arguments.
11 With all of that out of the way, let's go ahead and get the party appearances.
12 Who's appearing on Petitioner's behalf, please.

13 MR. DONOVAN: This is Gerard Donovan with Reed Smith for
14 Petitioner Keysight. And with me today is also Paul McDonnell from Reed
15 Smith.

16 JUDGE TURNER: And who will be presenting today? Is that
17 you, Mr. Donovan?

18 MR. DONOVAN: Yes, I will be presenting. Thank you.

19 JUDGE TURNER: Okay. And did you want to at this time
20 reserve any time for rebuttal?

21 MR. DONOVAN: I'd like to reserve 10 minutes.

22 JUDGE TURNER: Okay, gives you 35 principal. Okay. And on
23 behalf of Patent Owner.

24 MR. HANNAH: Good morning. Good afternoon, Your Honors.
25 James Hannah, on behalf of the Patent Owner. With me is Jeffrey Price, and

1 Jeffrey Price will be presenting today.

2 JUDGE TURNER: Mr. Price, did you want to reserve any time for
3 sur-rebuttal at this time?

4 MR. DONOVAN: Jeff, you're on mute.

5 MR. PRICE: I'm sorry. I'll also reserve 10 minutes, Your Honor.

6 JUDGE TURNER: Okay. Are there any questions or concerns the
7 parties want to raise before we begin, from either side? Okay. Not hearing
8 any, Petitioner, when you are ready you may begin.

9 MR. DONOVAN: Thank you. Paul, could you bring up the
10 exhibits? The demonstratives. There you go. Are you able to see the
11 demonstrative slides? All right.

12 May it please the Board. My name is Gerard Donovan and I
13 represent Petitioner Keysight Technologies. I'll be referring to Petitioners
14 demonstrative slides today, which were filed as Exhibit 1103. And as set
15 forth in the petition and the record, the claims of the '343 Patent are obvious
16 in view of the combined teachings of Sourcefire and the Emerging Threats
17 prior art references. Slide 2 of the demonstratives, of Petitioners
18 demonstrative, shows the language from claim 1. Could you go slide two?
19 Thank you. The prior '552 IPR established that Sourcefire's prior art to the
20 '343 Patent and that it teaches most of the claim elements. The Board's
21 decision the '552 IPR was affirmed by the Federal Circuit and its findings
22 are binding here. The disputes now focus primarily on claim element 1(e),
23 and specifically that configured to prevent an exfiltration operation claim
24 language.

25 And before I go into the disputes, for context, I want to briefly

1 discuss the teachings of the '343 Patent. The background of the Patent
2 asserts that there are several reasons why it's difficult to prevent
3 exfiltrations. For example, one of the reasons is that humans may engage in
4 network activities that are vulnerable to attacks. And we can go to slide 3.
5 The specification goes on to describe two exfiltration attacks and methods
6 for preventing them. It discloses that an attacker can exploit a known
7 vulnerability with TLS version 1.0 to decrypt messages in HTTPS sessions.
8 So, a human may think the connection's secure, but it may actually be
9 vulnerable to exfiltration using an out-of-date and insecure version of an
10 encrypted protocol. In an attempt to prevent such exfiltrations, the Patent
11 discloses a, quote, require TLS 1.1 or 1.2 operator that checks the TLS
12 version in an application packet header and then blocks packets that use TLS
13 1.0 and allows packets that use TLS 1.1 or 1.2.

14 The Patent separately discloses that attackers can use HTTP put or
15 HTTP post methods to exfiltrate data. And the Patent solution is the HTTP-
16 EXFIL operator, which checks the HTTP packet application headers and
17 allows packets that use the get HTTP method and blocks packets that use
18 other methods such as put or post.

19 Turning to slide 4. In the '552 IPR it was established that
20 Sourcefire discloses an intrusion prevention system or IPS that uses rules to
21 examine packets to determine whether to block, allow, or generate events.
22 As shown here Sourcefire also teaches importing rules. For example, you
23 can import a text file of Snort Rules. Sourcefire teaches that imported rules
24 are initially set to be disabled and a user must set the rule state of the local
25 rules before they can be used.

1 Now on slide 5, Emerging Threats was a leading provider of Snort
2 Rules back in 2010 and before that. Shown here on the left is Exhibit 1102,
3 which is a capture of the archived Emerging Threats web page from 2010. It
4 shows on the left links to navigate to the rules to search the website and to a
5 documentation wiki. From the rules link you can download the Emerging
6 Threats dash all rules file, which is Exhibit 1020, the Emerging Threats
7 reference in this IPR. On the righthand side is Exhibit 2016, which is an
8 archived page that you can access through the documentation wiki shown on
9 the left. And this also provides a different link to download the Emerging
10 Threats all rules file, which is again Exhibit 1020.

11 Moving to slide 6, in support of the petition, Dr. Staniford,
12 Petitioner's expert, explained that he personally was familiar with Bleeding
13 Snort, which later became the Emerging Threats project prior to 2010.
14 Some of his testimony from Exhibit 1003 shown here is from paragraphs
15 164 and 206. The petition also cited to Patent Owner's own 2014 press
16 release, recognizing Emerging Threats as the *de facto* standard in network-
17 based malware threat detection. While that press release itself postdates the
18 priority date of the Patent, it recognized the history of Emerging Threats
19 dating all the way back to 2003.

20 Turning to slide 7, testimony from Patent Owner's employee, Mr.
21 Marinho, confirms that Emerging Threats qualifies as a prior art publication.
22 Back when Mr. Marinho was a student and intern, he personally downloaded
23 Emerging Threats from his webpage that was in his exhibit, or in his
24 deposition, which is Exhibit 1101 at page 19. On page 20, he confirmed that
25 he had no trouble downloading it and that Emerging Threats was the most

1 well-known third party provider of Snort Rules at the time. It was the only
2 one he was aware of. On page 45 of Mr. Marinho's deposition, he also
3 confirmed that the rules that he downloaded was the emerging dash all rules
4 file, which is the Emerging Threats prior reference in this IPR, Exhibit 1020.
5 This testimony confirms that an interested artisan that prior to 2010
6 exercising reasonable diligence could easily locate and download the
7 Emerging Threats reference.

8 Now on slide 8, Emerging Threats includes numerous rules that
9 detect exfiltration operations. The example shown here examines outbound
10 traffic using SSL version 3.0. As Dr. Staniford explained in his declaration
11 in paragraph 267, he recognized this rule as attempting to find exfiltration's
12 of encrypted data or to prevent the loss of data using an outdated and
13 insecure version of SSL or TLS. In paragraph 229 of his declaration, Dr.
14 Staniford also observed this Emerging Threats rule was very similar to the
15 required TLS operator of the '343 Patent. They both detect out-of-date
16 versions of the SSL TLS protocol by checking the application packet header
17 values. But the Emerging Threats rule checks for SSL version 3, which is
18 even more outdated than TLS 1.0. Note that this rule shown here starts with
19 a hash or a number sign indicating that it was commented out in Emerging
20 Threats. In order to load this rule into an IPS, one would remove the hash
21 sign from the rule to enable it. Emerging Threats distributes many of its
22 rules like this and teaches a user of its rules to enable the rules that they wish
23 to use. The reason the rule is included is so that it can be loaded into a
24 system like Sourcefire, it's desirable to be used by a user.

25 Turning to slide 9, as I mentioned earlier, when the text rules are

1 imported into Sourcefire, they're initially disabled and the rule state must be
2 set. Slide 9 shows the interface where a user can select the rule state button
3 to set the rule state for rules that are important into Sourcefire. On the right
4 is an excerpt from page 438 of Sourcefire, which explains that one could set
5 the rule state to generate events, to drop traffic and generate events, or to be
6 disabled. Slide 10 shows some of Dr. Staniford's testimony explaining that a
7 person of ordinary skill in the art, using the Emerging Threats rule set with
8 Sourcefire, would enable rules and set them to drop once they observed that
9 they operated as desired. And that's in paragraph 268 of Dr. Staniford's
10 declaration. In paragraph 289, he explains that the obvious desirable effect
11 of setting a rule state to drop for a rule configured to detect outbound
12 packets using SSL version 3 that might well be exfiltration's. In other
13 words, it was desirable, it was known that it was desirable to prevent
14 exfiltration's from a network.

15 Now on slide 11, Patent Owner argues that the claims do not cover
16 rules that Patent Owner contends are overbroad or fail to preserve the flow
17 of legitimate traffic without disruption. Patent Owner has not sought and
18 expressed construction and argues in the sur-reply that no construction is
19 necessary. However, Patent Owner's arguments also maintain that the
20 Emerging Threats' rules do not teach the configured to prevent an
21 exfiltration operation because Patent Owner contends they're too broad.
22

23 Thus, Patent Owner's arguments, it depends on implicit
24 construction that gives the claim term a breadth or narrowness requirement
25 such that a rule doesn't block too much or possibly drop legitimate traffic

1 too.

2 Slide 11 shows, sorry, slide 12 shows another excerpt from Patent
3 Owner's sur-reply arguing that the prior art is insufficient because Patent
4 Owner argues that it would not preserve the flow of legitimate network
5 traffic without disruption. The first problem with Patent Owner's argument
6 is it has no support in the claims. The claims only recite applying a packet
7 transformation function configured to prevent an exfiltration operation. The
8 claims do not have a vague limitation regarding the preserving the flow of
9 traffic or the breadth of the exfiltration. The second problem is that Patent
10 Owner's tacit claim construction would exclude the embodiments disclosed
11 in the '343 Patent for preventing an exfiltration operation.

12 Turning to slide 13.

13 JUDGE TURNER: Counsel?

14 MR. DONOVAN: Yes.

15 JUDGE TURNER: Counsel, this is Judge Turner. If you can go
16 back to slide 12 for just a second. I guess if I understand that you're saying
17 that the Patent Owner is making an assertion, is making an implicit claim
18 construction. But doesn't this argument also find fertile ground in the fact
19 that whatever network device I have has to have some utility? So, if I have a
20 rule that blocks all traffic, you know, that's not a very good network device,
21 is it?

22 MR. DONOVAN: You know, I think claim construction disputes
23 need to be resolved in IPRs to the extent they bear on the analysis here. And
24 the prior art rules that we're pointing to are rules that are designed to prevent
25 exfiltration's. And so, it's not a question of whether a prior art system that

1 enabled blocking all traffic discloses this claim element. So, I don't think we
2 need to resolve the bounds, and I don't think that this claim would cover a
3 system that simply blocked all traffic, and therefore prevented exfiltration's.
4 But here, if I understand Patent Owner's argument, they're saying that the
5 source, sorry, the Emerging Threats' rules don't teach us claim element,
6 because they block some traffic that may not be exfiltration. So, they don't
7 sufficiently preserve the flow of legitimate traffic. And that is something
8 that I think goes beyond what the claims recite, and it goes beyond what's
9 disclosed in the specification. There we have two rules that look to specific
10 ways that exfiltration is mediated, one using an out-of-date encryption
11 protocol and the other using HTTP put, post, and other methods other than
12 GET, and broadly blocking those. And so, the methods that the Patent, the
13 '343 Patent discloses for preventing exfiltration, prevents exfiltration and
14 legitimate traffic alike if they're using those methods. And that's the same
15 thing that the Sourcefire and Emerging Threats reference disclose, except the
16 Emerging Threats is actually an improvement on this in that it does more to
17 preserve the flow of traffic than the Patent discloses because we do have
18 rules that are also checking URI content. We do have rules that are
19 preventing the triggering of the SSLv3 rule based on certain known higher
20 TCP ports. And so, here we actually have a prior reference that goes further
21 than the Patent for preserving the legitimate flow of traffic. And so, the
22 claim should not be construed to exclude this reference. Does that make
23 sense?

24 JUDGE TURNER: Yes. No, I understand the position, thank you.

25 MR. DONOVAN: Thank you. And on slide 13, so here, and this

1 goes to how I was answering that question, there are two rules that are
2 disclosed and two methods for exfiltration that are disclosed in the '343
3 Patent. One of them is the HTTPS method that looks at the TLS version and
4 excludes all traffic that has TLS version 1.0 and allows traffic with 1.1 or
5 1.2. Here, there is no provision for preserving legitimate traffic, whether
6 traffic's legitimate or not, if it's using TLS 1.0, it's excluded. And the other
7 method is the HTTP-EXFIL method. And that's going to exclude HTTP
8 packets. It looks at the application packet header for the HTTP method, and
9 it's going to allow packets that are using GET, and it's gonna block
10 everything else. It's gonna block HTTP PUT methods, HTTP POST
11 methods. And so, it doesn't look at what traffic is legitimate or what traffic
12 is not. It's gonna block all traffic that's using those HTTP methods without
13 regard to the flow of legitimate traffic. So, in some, Patent Owners'
14 arguments would exclude those embodiments to the extent they excluded the
15 Sourcefire and Emerging Threats references.

16 Turning to slide 14, Patent Owner also contends that the Emerging
17 Threats SSLv3 rule does not teach detecting an exfiltration operation.
18 However, as Dr. Staniford observed, this rule is essentially the same as the
19 one, one of the two rules disclosed in the '343 Patent for preventing
20 exfiltration operations. This rule checks the application header for the TLS
21 or SSL version, and then it blocks, or it's triggered for packets that use SSL
22 version 3, which is an even earlier version of SSL TLS than TLS 1.0. This,
23 in combination with the Sourcefire reference which can set rules to block
24 teaches the elements of the claim.

25 Now on to slide 15, Dr. Staniford confirms that the Emerging

1 Threats SSLv3 rule would be triggered by such exfiltration operations. He
2 explained that the Emerging Threats rule looked for data going out in a
3 weird way using an unusual port and using a very old encryption protocol.
4 And he explained that that's basically the same technique for detecting
5 exfiltration's that he used when he worked at FireEye. So, he recognized it
6 as an exfiltration operation.

7 Turning to slide 16, Patent Owners employee, Mr. Marinho
8 confirmed in his deposition that this rule would be triggered by malware
9 exfiltrating data as well as other traffic. And again, this is just like the rules
10 in the '343 Patent itself that block exfiltration and legitimate traffic alike if
11 they're using the TLS 1.0 protocol. Patent Owner's expert also admitted that
12 the rules would be triggered if exfiltration is being performed using SSLv3
13 on a high port. And Dr. Goodrich's testimony is here on the right. And in
14 his answer, he says, "if a packet is using SSL on a high port that is not
15 excluded, then it will alert." And he qualified his answer about a high port
16 not being excluded because Emerging Threats includes many rules before
17 the SSLv3 rule. They create exceptions to preserve the flow of traffic on
18 high ports that are known to be likely legitimate traffic. So, the Emerging
19 Threats rule is actually more capable than the rule disclosed in the '343
20 Patent. And even if the claims were construed to require some preservation
21 of the flow of legitimate traffic, Emerging Threats teaches this claim
22 element.

23 Now on to slide 17. The Patent Owner also argues that this rule
24 doesn't prevent an exfiltration operation because distribution list
25 communication references working on a string of Emerging Threats

1 signatures to identify good TLS or SSL sessions because there's a bot using
2 standard SSL for command and control sessions on a high port. First off,
3 Patent Owner's argument fails because the question is what the Emerging
4 Threats reference itself teaches to a person of ordinary skill in the art. As
5 we've discussed, it teaches detecting exfiltration operations and the
6 motivation for its creation is not controlling. However, if you do look to the
7 motivation, that reinforces that this rule is designed to detect exfiltration's
8 while preserving the flow of legitimate traffic. The rule is to catch a
9 command and control session on a high port, and Mr. Marinho testified,
10 malware would communicate with a command and control server to
11 exfiltrate data. And that's in Exhibit 1101 at page 18.

12 In his deposition, Dr. Staniford also explained that a popular thing
13 for a trojan to do is upload data from browser forms to a command and
14 control server, which is a trojan exfiltrating data. The signatures or SIGs
15 referenced here in the, quote, good SSL or TLS sessions are the many SIGs
16 before the SSL version 3 rule in the Emerging Threats reference that identify
17 high ports known for legitimate traffic and exempt them from the SSLv3
18 rule. Thus, not only does the SSL version 3 rule detect exfiltration
19 operations, but when writing context of the other rules in this posting, it does
20 so while preserving the flow of traffic. There are many other rules in
21 Emerging Threats that also target exfiltration operations while preserving the
22 flow of legitimate traffic.

23 Slide 18 shows a rule that checks for an application header field
24 value with HTTP POST methods, just like the HTTP-EXFIL rule in the '343
25 Patent. And the message of this rule indicates that it's looking for a spyware

1 check-in. As Dr. Staniford noted in his deposition, and this is shown at the
2 bottom right here, the reference to spyware certainly suggests that this rule is
3 detecting software capable of exfiltrating data.

4 Slide 19, next, includes testimony from Patent Owner's employee,
5 Mr. Marinho, confirming that this rule checks an application header field
6 value for an HTTP POST method. And when asked what spyware is used
7 for, he explained, quote, so spywares were designed to actually spy, collect
8 information on the system, and exfiltrate it. And that's in his deposition
9 transcript at page 110. So, clearly this is another rule designed to detect
10 exfiltration attempts by checking application header field values. This rule
11 also checks for URI content known to be associated with spyware. Thus,
12 this rule better preserves a flow of legitimate traffic than a rule that simply
13 blocked all traffic using HTTP POST methods. In other words, the '343
14 Patent discloses a rule that simply looks at the method in the application
15 header and blocks legitimate traffic and illegitimate traffic alike using HTTP
16 POST methods. And this rule, in addition to checking for the HTTP method
17 in the application header, is also checking for resource information, the URI
18 content, to determine whether it's likely associated with spyware.

19 Turning to slide 20, I'll just quickly note that this is another
20 example rule that's triggered by exfiltration operations detected by checking
21 application headers for HTTP POST and URI content associated with
22 malware. Again, this rule is just like the HTTP-EXFIL rule in the '343
23 Patent, but it's better at preserving the flow of legitimate traffic because it
24 checks for specific URI content instead of just blocking all HTTP post
25 packets.

1 Slide 21 has testimony from Mr. Marinho confirming that the rule
2 is triggered after checking the application header field values, and that the
3 rule is designed to detect outbound traffic from malware to a command and
4 control server, a reason for which would be to exfiltrate data. Now, Patent
5 Owner argues extensively that a person of ordinary skill in the art would not
6 have found it obvious to set the Emerging Threats rules to block once
7 imported into Sourcefire. And this argument attacks Emerging Threats
8 reference alone, and the petition identified Sourcefire's teaching of enabling
9 the rules and Dr. Staniford's testimony explaining that an ordinary artisan
10 would be motivated to tune rules and enable them based on their network
11 environments and would have seen an obvious desirability of blocking
12 malware that's exfiltrating data.

13 Dr. Staniford also explained that, well, Dr. Staniford explained that
14 in paragraph 233 of his declaration when he said the Emerging Threats rules
15 leave a person of ordinary skill motivated to block exfiltration's using these
16 Snort Rules with Snort-based systems such as for Sourcefire. And that was
17 in the petition at page 37. So, even if it wasn't obvious to block malware
18 from exfiltrating data, a skilled artisan with knowledge of Sourcefire and
19 Emerging Threats would have found it obvious to try setting the rules for
20 detecting malware to block rather than just alert. Specifically, when
21 Emerging Threats rules are imported into Sourcefire, a user has the options
22 to disable the rule, set the alert to block, or set, or sorry, set the rule to alert
23 or set the rule to block. And these are limited options with predictable
24 results and they're all obvious.

25 Patent Owners' secondary consideration arguments do not

1 overcome the strong showing of obviousness here. Here, the prior art
2 references include express teachings supporting their combination.
3 Sourcefire teaches loading text files of Snort Rules and setting the rule
4 states, and Emerging Threats is a text file of Snort Rules that are designed to
5 be loaded into a cybersecurity system such as Sourcefire. No secondary
6 consideration could overcome the strong showing of obviousness.

7 Patent Owner's secondary consideration arguments should also be
8 given no weight because they lack the requisite nexus to the claims. Patent
9 Owner's arguments refers to analysis of secondary considerations in prior
10 challenges to related Patents. Those didn't deal with the obviousness case
11 that's presented here. None of those addressed the combination of
12 Sourcefire and the Emerging Threats rules teaching rules that are triggered
13 by exfiltration operations.

14 Moving to slide 22. Dependent claims 5 and 12 require allowing,
15 based on a determination, that the application header field value indicates a
16 request for specified resource data. The petition showed that Emerging
17 Threats teaches a rule that detects an exfiltration operation and checks an
18 application header field value for URI content to determine whether to allow
19 or block the packet. And the URI is a uniform resource identifier. So, the
20 rule is checking if the application header in the packet indicates a request for
21 a specific resource, which is exactly what the claim requires. In Patent
22 Owner's response, Patent Owner argued that Emerging Threats didn't teach
23 this claim element because it didn't analyze application header field values.
24 That argument fails because, as shown in the petition, the rule checks the
25 application header field value for the URI content. That's where the URI

1 content is, is in the application header. Mr. Marinho admitted this in his
2 deposition that the rule checks the application header field values for URI
3 content.

4 Turning to slide 23. In Patent Owner's sur-reply, Patent Owner
5 advanced a new argument that the URI is not specified resource data. Patent
6 Owner argues that, as used in the '343 Patent, resource refers to the parties in
7 a communication session, which are identified by the 5-TUPLE Data. And
8 to support that, Patent Owner refers to some references to resource in the
9 specification. This new argument fails for a few reasons. First, because it
10 was waived and not timely raised in Patent Owner's response. But on the
11 merits, it also fails. Its argument is based on an implicit construction that's
12 contradicted by the claims themselves. The 5-TUPLE information in
13 packets is found in the communication session in the packet header. So, the
14 TCP packet and the IP packet header has the information for the IP
15 addresses, the protocol on the ports. Claim 5 is checking the application
16 header, which does not include the 5-TUPLE information. So, Patent
17 Owner's construction can't be meshed with the claims themselves that are
18 checking the application header values. Further, the claims are explicitly
19 referring to specified resource data. They're not referring to the parties to a
20 communication session. That's earlier in the claims when you're checking
21 the TCP packets. And so, the Emerging Threats rules do check the
22 application header field values for uniform resource identifiers, which
23 identify the specific resource data that's being checked. So therefore, the
24 Emerging Threats rules disclose this additional claim limitation of dependent
25 claims 5 and 12.

1 With that, unless the Board has any questions, I'll reserve the
2 remainder of my time.

3 JUDGE AMUNDSON: This is Judge Amundson. I had a question
4 about Mr. Marinho and Keysight is relying on his testimony in part to show
5 the public accessibility of Emerging Threats. So, my question is, did Mr.
6 Marinho indicate how he became aware of the Emerging Threats?

7 MR. DONOVAN: Yes, he did. I'd have to pull up those sites from
8 our reply brief. But he was a member of a distribution list for Snort Rules
9 generally. And the Emerging Threats team would post on the Snort's rule
10 distribution list. So, Snort was a well-known standard for rules for IPS's,
11 IDS's in the '90s and 2000s. And so, while he was both a college student and
12 an intern, he was on this distribution list to learn about Snort rules generally.
13 And that's where he saw the Emerging Threats team posting about the rules
14 that they distributed. Through that, he also joined the Emerging Threats
15 distribution list and was aware of their website and downloaded it.

16 JUDGE AMUNDSON: All right. Thank you.

17 MR. DONOVAN: You're welcome. I also want to address part of
18 the premise of your question. We are citing to that to counter Patent
19 Owners' arguments that Emerging Threats was not sufficiently available in
20 the prior art. However, the petition did show the archived webpages and
21 provided Dr. Staniford's testimony regarding the availability of first the
22 Bleeding Snort project and then Emerging Threats, as well as the Patent
23 Owner's publication or press release about the prevalence of Emerging
24 Threats and the history of it.

25 JUDGE AMUNDSON: All right. Thank you.

1 MR. DONOVAN: Thank you.

2 JUDGE TURNER: Thank you, Mr. Donovan. You will have 18
3 minutes when you choose to use it for rebuttal. We're going to go ahead and
4 turn to Mr. Price. You may present the Patent Owner's response hereto.

5 MR. PRICE: Thank you, Your Honor, and may it please the
6 Board. I'm just going to share my screen here. Just let me know that
7 everyone can see that.

8 JUDGE TURNER: Yes.

9 MR. PRICE: Okay. So, before I begin, I just want to thank Your
10 Honors for taking the time here today to really dive into the record here
11 because this is a very important Patent, very important technology for our
12 client. And this is a technology, you know, that we're on maybe the fourth
13 challenge to one of the Patents in this family of Patents for exfiltration.
14 There were two IPRs earlier filed against the related '193 Patents. There was
15 an ex parte re-examination of the '193 Patent. And there was an earlier
16 challenge by another party, well, the Pan Palo Alto Networks who has been
17 joined to this proceeding. That was also unsuccessful. And the key thing
18 that's been consistent across all of these cases and all of these decisions is
19 that it wouldn't have been obvious to modify Sourcefire, which is an
20 intrusion prevention system to block exfiltration operations. And there are a
21 number of reasons for that. So, here I'm on page 2. The background of the
22 invention talks about why exfiltration, different from intrusions, had been
23 proven especially difficult for conventional cyber defense systems to
24 prevent. And a lot of the reasons were that prior attempts to address the
25 exfiltration problems were too coarse, overbroad, and they resulted in a large

1 negative impact on the networks employing these exfiltration prevention
2 techniques. As Your Honors are aware from reading specification. Of
3 course, any person of ordinary skill in the art could block an exfiltration by
4 just shutting down all traffic to a system. That would do the trick. But that's
5 not what Centripetal did. And that's not what anybody would have done,
6 right? So, what is Centripetal do? They came up with a solution to the
7 exfiltration problem that would prevent exfiltration while still preserving the
8 flow of normal legitimate traffic without disruption.

9 Before I go much further, I think it would be helpful here to talk
10 about the non-claim construction issue in this case. There is no claim
11 construction issue. There's no requirements in the claims for some level of
12 protection, you know, that some subjective kind of feeling about what the
13 flow of normal legitimate network traffic without disruption means. We're
14 not trying to read any limitations into the claims themselves. Instead, why
15 do we bring this up? It's because if you would turn, if a person would have
16 turned on any of these Emerging Threats rules on an IPS device like
17 Sourcefire, they would have run into major problems. And both Dr.
18 Goodrich, Dr. Staniford, and Mr. Marinho, all are in agreement that you
19 cannot turn on a rule that has adverse, too much of an adverse effect on your
20 network. And the key, the number one non-obviousness argument we're
21 making here today is that Emerging Threats doesn't teach any drop rules.
22 Every single rule in Emerging Threats is an alert rule. And it's an alert rule
23 for a very good reason, which Mr. Marinho talked about at length during his
24 deposition. Mr. Marinho, as you may be aware, was contributed to
25 Emerging Threats -- worked for Emerging Threats. And his testimony is

1 very clear that these Emerging Threats rules are not IPS rules. They are IDS
2 rules. They are intrusion detection system rules. They are not intrusion
3 prevention system rules. And the idea that just because Sourcefire says that
4 you could turn on, you know, change the action of a rule from alert to drop
5 is not motivation to modify any of the Emerging Threats rules, let alone the
6 specific rules identified in the petition in order to begin dropping traffic.

7 So, with that introduction, turning to page 3.

8 JUDGE TURNER: Counsel.

9 MR. PRICE: I'm sorry, go ahead.

10 JUDGE TURNER: Counsel, this is Judge Turner. If maybe we
11 can just sort of explore that for just a second. Hopefully, I won't take up too
12 much for your time. But one would think that if I have a rule that causes
13 alerts, that that would be it would be very obvious to say okay well I'm
14 going to do something about that, you know, if I'm running a network device
15 and I'm getting, you know, hundreds, thousands of alerts maybe it would be
16 obvious therefore to say okay let's do something about that. Let's drop
17 packets, or let's, you know, shunt packets somewhere else so that -- why
18 wouldn't it be obvious if you have a rule that's going to alert you of a
19 potential problem to act on it?

20 MR. PRICE: Sure, Your Honor. And I obviously I was gonna get
21 to that in more detail later but while you asked the question I'm happy to
22 answer it now. There are umpteen reasons and including a lot of disputed
23 evidence from both Dr. Goodrich and Mr. Marinho that these rules are for
24 one, they are meant specifically to detect intrusions. And what these
25 systems were doing at the time of the invention, intrusion detection systems

1 and intrusion detection rules, they would analyze traffic offline to
2 understand what kind of traffic was on the network. And you would have
3 teams of network analysts who would look at the alerts to understand
4 whether or not something is occurring on your network that you don't want
5 to. Why wouldn't you turn a rule on for drop? There are, number one,
6 performance. Any of these rules that do string searches for your eye content,
7 for any information in the text of the communications, doing string searches
8 like that are very, very computationally expensive. And so, what does that
9 mean? They take too long to evaluate these rules against traffic in real time.
10 So, and you need to do this in real time in order to block the traffic. So,
11 number one reason that you wouldn't turn any of these IDS rules on is that
12 they're too expensive. And they're meant to be expensive, right, because
13 they're meant to be looking for very, very specific exploits, known malware,
14 virus signatures, these kinds of things are not -- you can't put them into
15 effect at the edge of your network to block traffic. This is well known. It's
16 not -- it's just not disputed in the record. And to the idea that well, you
17 know, there are only three options, right? You can block, you can drop, you
18 can pass, or you can alert. Why wouldn't it have been obvious because you
19 would have destroyed the usability of these machines. And that's what Mr.
20 Marinho says. He was horrified to hear that somebody was trying to make
21 the contention that you would have put these rules in effect on live traffic
22 and actually drop them when that was never ever the intention of these rules.
23 So, you know, performance is one reason. You know, and so my friend
24 says, well, you know, a person of ordinary skill in the art would download
25 this, you know, list of 11,000 rules. Just put them into effect on the

1 Sourcefire appliance and look at them and decide whether or not they're
2 acting as appropriate, and then you can decide to drop them. That's to
3 change them to drop. Well, first of all, it doesn't deal with the performance
4 issue. No person of ordinary skill in the art would have turned on any of
5 these rules because of performance issues. But what else, what did my
6 friend not say? He did not say that he or his expert or anybody else who's
7 making, you know, this obviousness argument had actually evaluated. What
8 would happen if you turned on any of these rules? Now let me -- that's very
9 important, very important, because what did several of the earlier cases
10 about exfiltration say? Yes, it looks like Sourcefire could be modified in
11 order to reach the claims of the '193 Patent, for example. But a person of
12 ordinary skill in the art would not have done so. And this, you know, this
13 key legal principle is about what a person of ordinary skill in the art would
14 have done, not what they could have done. So, the fact that a person of
15 ordinary skill in the art could have downloaded this, could have loaded the
16 Emerging Threats rules, could have loaded them into Sourcefire, could have,
17 I suppose, looked at the performance of every single one of those 11,000
18 rules and decided, yeah, I want to turn this one on, I want to turn this one
19 off. No person of ordinary skill in the art would have done that is what the
20 undisputed record shows in this case. But more specifically, there is no
21 motive -- there's no, not even an argument, let alone evidence that any
22 person of ordinary skill in the art would have turned on, for dropping
23 purposes, any of the rules identified in the petition or in their reply.

24 JUDGE TURNER: This is Judge Turner. Let me try again. So,
25 this hypothetical. So, let's say we have Sourcefire, and we introduce all of

1 these rules. I'm assuming that if they are set up purely for alert and not for
2 drop, that's not going to create a performance problem. Is that correct, or is
3 it still going to?

4 MR. PRICE: That's correct.

5 JUDGE TURNER: Okay. So --

6 MR. PRICE: And let me answer why. The way that Sourcefire
7 works is it will -- for each packet that comes in, it recognizes the packet as
8 part of the session. It puts all of the information and all the packets in the
9 session together and then runs it on the set of rules. Now, that will happen,
10 and your traffic will just go. If it's an alert rule, it's not going to hold off the
11 traffic in order to wait for the analysis to be done, because, again, the whole
12 point of an IDS device is it's not going to -- an IDS device and these IDS
13 rules is there for informational purposes to understand what's happening on
14 your network. They are not for drop in traffic. And I can't reiterate this
15 enough is that Emerging Threats is an IDS rule provider. Mr. Marinho was
16 an IDS rule writer. He testified that he didn't write rules for IPS devices and
17 that the rules that any person of ordinary skill in the art would recognize
18 these rules as IDS rules that are used in a very, very different way than the
19 Petitioner is trying to claim that they would be used in conjunction with
20 Sourcefire.

21 But again, you know, what I need to reiterate this, again, because
22 it's so important that just because you could have gone in and turned on any
23 of these rules does not mean that you would have. And there is no evidence,
24 no evidence in the record that any person of ordinary skill on the art would
25 have found it reasonable to turn on any of these rules. What we have

1 instead, we have a general statement that a person of ordinary skill in the art
2 would want to block malicious traffic and would turn on these rules. But
3 that doesn't get into any of the other reasons why you wouldn't have turned
4 on any of these rules to begin with. And that's not even getting into --

5 JUDGE TURNER: Counsel? Counsel?

6 MR. PRICE: Yeah, I'm sorry.

7 JUDGE TURNER: Oh, no, thank you. Thank you. I appreciate
8 your answers are a little bit verbose, but I'm trying to -- with respect to the
9 hypothetical. So, I'm assuming, I think you said yes, that if we put these in
10 and all they do is create an alert, there's no performance hit. I think you said
11 yes to that. But I guess that that does raise the question that if I'm running
12 my system, my network device, and I've got all these alerts, why wouldn't it
13 be obvious to one of ordinary skill in the art to say, gee, I've got an alert here
14 that says that I have an exfiltration problem, why wouldn't I want to, you
15 know, act responsibly to that? Why wouldn't, even if I assume what you're
16 saying is, okay, I brought them all in, I'm creating all these alerts because of
17 all these rules and I've got them all commented out and they're not
18 interfering with traffic, but once I get all the alerts, why would I not say,
19 well, why don't I take some, you know, response in order to prevent it? Why
20 wouldn't that be a logical, you know, progression from having the alerts?

21 MR. PRICE: Right. So, again, false positives are going to be a
22 major problem. We didn't get into false positives earlier. We were just
23 talking about performance. But false positives are a major problem. So,
24 what these rules are made for is to, for example, catch an encrypted session.
25 This is the main rule that we're talking about in the petition is about catching

1 an encrypted session on a high port. And why are you doing that? You're
2 doing that because there is an instance of a bot, an exploit, some malware
3 that happens to send traffic on a high port. So, a rule was written to say,
4 well, you know, if there's some traffic, encrypted traffic going on -- on a
5 high port, you should look at this. And the network administrator will look
6 at it and say, yeah, actually, this was an instance of the bot. Let's, you know,
7 clean that computer. Let's delete it. Let's make sure that, you know, we
8 address it and take some countermeasures. That doesn't mean that a person
9 of ordinary skill in the art would turn that rule on as a drop rule, right?
10 Because for every one instance that, you know, there was a bot detected, you
11 might have 100 that were completely denied, right? So, the question is, you
12 know, why, what are these rules for? They're for understanding what's
13 happening on your network, letting the network administrators know, but
14 they're not for detecting traffic up front. They're not for blocking traffic.
15 And they -- and again, there is no, none, evidence that any one of these rules
16 would have operated as desired. All they have -- all the Petitioner has said is
17 that a person of ordinary skill in the art could have done this. But they didn't
18 say that they would have done it for any of the rules that we are considering
19 in this case. They have not met their most fundamental burden.

20 JUDGE TURNER: This is Judge Turner. Just as a quick follow-
21 up, I'm assuming that in respect to the '343 Patent's methods, I'm assuming
22 there could be legitimate traffic that might use HTTP PUT or POST, and
23 that under the Patent's system, those would be blocked, so it would block
24 legitimate traffic and it could, you know, in theory, if I have a bunch of
25 traffic or, you know, particular applications or something that are using, you

1 know, such commands, I could really slow down my network device even
2 through the Patent processes, too, as well. Could I not?

3 MR. PRICE: No, Your Honor. So, the key difference and what
4 Centripetal did really to solve this problem was they're using information
5 about the networks, the resources that are talking to each other. So, back to
6 page 3 where we're talking about determining that a packet has a packet
7 header field value with the first portion of packets. This is talking about
8 Centripetal's use of cyber threat intelligence. What's going on here is you
9 look at the 5-TUPLE Data, and by looking at that and in conjunction with
10 your cyber threat intelligence data, right, these are how these rules are being
11 generated, and you know we could take a look. Let me see if I can do this.
12 Do you now see the '343 Patent?

13 JUDGE TURNER: Yes.

14 MR. PRICE: So, my friends want to make this case all about the
15 application layer header information. But what makes the application layer
16 header information usable in Centripetal is that you are doing a first cut on
17 the source IP address and destination IP address. This is what we're talking
18 about when we're looking for location packet header field. So, you are able
19 to say, yes, I want to allow everyone on my network to send any -- post
20 anything to trusted networks, you know, network A, network B is, you
21 know, how the chain was specification. And I only want to apply this, you
22 know, for example, the EXFIL. New traffic, TCP traffic going from source
23 IP address 140, 210. And then it's a wildcard to anything with an IP address
24 starting at 213. So, this is what it has allowed Centripetal to say, look, we're
25 not going to apply these rules to all traffic, you know, like my friend said in

1 his introduction that it would block a post on every single, you know, packet
2 that came through and that's just not correct. So, that's, you try, you know,
3 they're trying to read a claim limitation in isolation without looking at the
4 claim as a whole. You know, obviously our arguments in the record were
5 mostly about the -- the application layer header data, but we can't forget
6 about, you know, what the packet header data is for and what Centripetal did
7 with this data in order to help solve this exfiltration problem because those
8 are two key pieces of the solution.

9 JUDGE TURNER: Okay.

10 MR. PRICE: So, I hope that answers the question and you know,
11 this was actually one of the reasons that the '193 Patent was found
12 (INDISCERNIBLE) over and over again is that, you know, this is really
13 talking about we're not, we're not applying -- we're not blocking all posts.
14 We're not a block, you know, we're not allowing all guests, for example.
15 But what we are doing is we're saying for this subset of data that we've
16 highlighted the first plurality of packets. We are going to restrict the ability
17 to post.

18 JUDGE TURNER: And this is Judge Turner. Just to be clear, I
19 making sure that I understand the argument. Patent Owner is not disputing
20 that Sourcefire would teach this aspect, I think it's 1(c). You're just saying
21 that the result would be different because you have these layers, and
22 therefore, yeah, you know, requiring the elements of 1(e), it wouldn't stop
23 traffic. Is that a proper paraphrase of your argument?

24 MR. PRICE: I think more to the point that this is all about whether
25 or not you're going to change an alert rule to a drop rule. Okay. So yeah,

1 we would say that in the prior art, given what Sourcefire teaches, given what
2 Emerging Threats teach, you would have to have a solution like this, with
3 what you're doing with the packet header data in order to make this a usable
4 rule in line for dropping traffic. And, you know, that's one of the things that
5 helps Centripetal solve this problem. It's not suggested anywhere in the art.

6 JUDGE TURNER: And I understand that. But I guess the
7 question is since Patent Owner is estopped from saying that Sourcefire
8 doesn't actually perform this, wouldn't the system of the proposed
9 combination also have the same benefit?

10 MR. PRICE: Well, no, Your Honor, because we're talking about
11 very specific rules in Emerging Threats. And this is a point that we made in
12 our papers is that if you are taking these, you know, other limitations from
13 Sourcefire, you need to then put those things together in a rule with what
14 Emerging Threats is doing. There's no discussion about modifying any of
15 the Emerging Threats rules with the other limitations that were known or,
16 you know, were known from Sourcefire, right? That's not what the
17 argument is. The argument is that Sourcefire can, you know, do a couple
18 things and then you would have Emerging Threats, teaches some rules that,
19 you know, if enabled would prevent exfiltration's. Our point is that first of
20 all, none of these Emerging Threats rules would prevent exfiltration because
21 there were alert rules. And you would not, a person of ordinary skill in the
22 art would not have implemented these as drop rules. But barring hindsight
23 and barring the solution that Centripetal brought to the table, which was the
24 ability to apply these rules based on their cyber threat intelligence that will
25 enable them to have these rules that are not over broad and that a person of

1 ordinary skill in the art would turn on the system and that now are
2 commonplace.

3 JUDGE TURNER: Thank you. I'll let you get back to your
4 discussion. I wasn't going to use up all your time and unfortunately, I think I
5 could use quite a bit of your time. I'll let you get back to what you'd like to
6 present, Mr. Price.

7 MR. PRICE: Yes. So, continuing on that point, I'm on page 10
8 now. Many of the rules in Emerging Threats are commented out, and rules
9 that are commented out, they're disabled using this pound or hash character,
10 well known that these kinds of rules would be commented out for having
11 excessive false positives or poor performance. And so, the question is, if
12 you have a rule that has excessive false positives and would destroy the
13 performance of your system, would a person of ordinary skill in the art have
14 made that into a drop rule? That's the question in this case. And the answer
15 is no. The fact that you could have is not sufficient for obviousness. And
16 again, there is no evidence in the record that Keysight tried these rules, tried
17 to implement them on an IPS device in the way that they suggest. There is
18 no evidence that for any of these specific rules, that a person of ordinary
19 skill in the art would have turned them on. Petitioner's arguments amount to
20 an allegation that a person of ordinary skill in the art would have turned
21 them on.

22 On page 11, and yeah, this is not a trivial change. So, here's Mr.
23 Marinho, these kinds of rules were never designed to drop traffic. He
24 knows, he wrote the rules. These rules exist to give evidence that some
25 network administrator can correlate events on the network with other events

1 in order to start an investigation. Prior to Centripetal, prior to their
2 inventions here, this is how things worked. This is how things worked in the
3 art. These were IDS rules, therefore intrusion detection. They are used to
4 determine whether or not a problem is on the network and let you start an
5 investigation. They do not, they were never meant to, and they were not
6 supposed to be turned on for dropping traffic. Petitioner's expert, Dr.
7 Staniford, acknowledged the problem with false positives. If a product has a
8 lot of false positives, it becomes unusable. A person of ordinary skill in the
9 art would not have turned on a rule that made the device unusable. It didn't
10 drop traffic in its original form, right? Petitioner needs to show that a person
11 of ordinary skill in the art would have modified it. But if it's going to have a
12 lot of false positives, you wouldn't have modified it, as claimed. And there's
13 no dispute over Mr. Marinho's testimony on this point. There is none.
14 Petitioner doesn't discuss it in their reply. They don't dispute it. And that,
15 Your Honors, is the crux of the case, is that these rules would never have
16 been turned on, and Petitioner has not even made out of their allegation that
17 any of these specific rules would have been.

18 The key rule that I think, you know, we're focused on in this case,
19 you know, there were four rules set in the petition. Three of them, I think
20 Your Honors recognized during an institution, don't even look at
21 application-like their data at all. The rule I think that parties are most
22 focused on is this rule 2003-021. And what does this rule do? It detects
23 encrypted data on a high port. Now, my friend during his opening
24 presentation spoke a lot about how you actually had to read this rule in
25 context with other rules. And so, let's do that, because when you do that,

1 and you look at the other rules in this set of rules, you'll see that this rule had
2 nothing to do with detecting encrypted data transmitted over an outdated
3 SSL protocol, which is the basis for Petitioner saying that, you know, this is
4 an exfiltration rule because there were some known vulnerabilities with
5 some older versions of SSL and TLS. However, if you actually look at the
6 (INDISCERNIBLE) in context, there are -- you know, I just want to make
7 sure I get the quote right. The Emerging Threats reference, the author of
8 these rules says it's not just about SSLv3. It -- "it's set to get SSLv2, SSLv3,
9 and most TLS implementations," because this rule is not about you know,
10 blocking traffic on, you know, with outdated SSL encryption protocols, it's
11 specifically to get a bot, right? And Dr. Staniford, you know, he very clearly
12 claimed that this was not, you know, designed for to, you know, track -- a
13 particular exploit, but that's exactly what it is. This is not about blocking an
14 exfiltration operation, it's about detecting a bot. And it's about detecting a
15 bot no matter what version of TLS or SSL is being used here.

16 JUDGE TURNER: This is Judge Turner. You have about three
17 minutes until you go into your rebuttal time.

18 MR. PRICE: Thank you.

19 JUDGE TURNER: Thank you.

20 MR. PRICE: So then moving on page 16, like I said, there were a
21 few other Emerging Threats rules cited in the petition. None of them were,
22 you know, looked at application layer header data. I don't think that there's
23 any dispute over those.

24 We move on to claims 5 and 12. So, claims 5 and 12 are about
25 allowing, based on a determination that the application header field value

1 indicates a request for specified resource data. Now, what is specified
2 resource data? Is, you know, is the first question here. Petitioner didn't, you
3 know, propose a construction for it. However, the specification is very clear
4 about what specified resource data is. A resource is a computer. And so,
5 you're looking for specific data on a computer. Now, during the opening
6 remarks, obviously my friend made a new argument because this wasn't in
7 the record. However, he said that you can only identify a resource based on
8 the 5-TUPLE Data. However, that's one way to identify a resource but that's
9 not the only way. And if you look at our sur-reply, well when we're talking
10 about these claims. The evidence shows that you find the resource data if
11 you have the full URI. Right. The full URI would say and
12 HTTP://www.(INDISCERNIBLE).com, and then slash, whatever the
13 resources that you're looking for. Now, the specific data I'm sorry that
14 you're looking for, the resource is the name of the computer. That resource
15 information is just not in this rule. What do you have in the URI content for
16 that they're pointing to claim 5. It's just a stub of a file then. It doesn't
17 identify the resource. So, if you're talking about, you know, specified
18 resource data, that's not what you get when you're looking at this UI content.
19 If the URI content had the full URI that identified the resource and the data,
20 then that would satisfy the claim limitation, but without the resource
21 identification. Right? Resource is a well-known term of art. It's used up
22 and down the specification. If you don't have the resource information and
23 you don't based on this URI content team rule they're pointing to, then you
24 don't have specified resource data.

25 Just touching briefly on the secondary considerations. Long felt

1 need and industry praise. These are -- this evidence is in the record now.
2 My friend wants to claim that there's no nexus. However, as we put forward
3 in the papers, you know, this idea that you're going to be using CTI, right,
4 this cyber threat intelligence as your first cut, right, is what helps Centripetal
5 solve this problem. And that has a nexus right there, the very first limitation
6 of the claims. And again, industry praise, a ton of it praising Centripetal is
7 the use of CTI for that purpose.

8 And then just briefly I'll touch on the Emerging Threats is not a
9 printed publication. Now, the standard for printed publication is that a
10 person of ordinary skill in the art using reasonable diligence and locate it.
11 Mr. Marinho was not, you know, we would claim that he's exercising more
12 than reasonable diligence. You know, he got himself, you know, involved in
13 a community that had a mailing list and he was on that mailing list, and it
14 was, you know, it was -- he had this mailing list that he first kind of heard
15 about Emerging Threats. And then, you know, he had to go to the website
16 and then, you know, click down through several levels of links. There was
17 no, you know, evidence that Emerging Threats was indexed. There was no -
18 - there's no evidence that a person of ordinary skill in the art searching for
19 keywords, right, related to the subject matter of this Patent for exfiltration
20 ever would have found emerging threatsEmerging Threats. But beyond that,
21 this is a file of 11,000 (INDISCERNIBLE). And each, pages 42 through 45
22 of our -- of Patent Owner's response, cites the *Portis v. Boston Scientific*
23 case. And what *Portis v. Boston* says is that a person's interested in ordinary
24 skills in the art must be able to, quote, recognize and comprehend therefrom
25 the essentials of the claimed invention without further research or

1 experimentation. What do we not have from Petitioner? You don't have any
2 evidence that a person of ordinary skill in the art, looking at the Emerging
3 Threats rule set would have recognized any of these rules as being designed
4 to prevent exfiltration's. What we have instead, and what the record shows
5 is that Petitioner looked at the '343 Patent, found rules that mapped on to
6 Centripetal's claims, and then when plumbing this document full of 11,000
7 rules to find ones that look somewhat like Centripetal's rules and
8 specification. That's hindsight. And it violates *Portis v. Boston Scientific*.

9 So, with that, Your Honor, unless there are any questions I will
10 reserve the rest of my time.

11 JUDGE TURNER: It doesn't appear that the panel has any
12 additional questions. Patent Owner, you will have six minutes for sur-
13 rebuttal when you come back on this. Mr. Donovan, you have 18 minutes
14 for your rebuttal. You may begin when you're ready.

15 MR. DONOVAN: Thank you, Your Honors. I kind of want to
16 reference the prior challenges to related Patents in this family and the prior
17 challenge to this Patent. Those prior challenges did not address the issues
18 here and the combination of Sourcefire with Emerging Threats. He argued
19 that there was no motivation to modify Sourcefire and those prior IPR is an
20 ex parte re-exam. It simply did not analyze the same record we had here and
21 the teachings of Emerging Threats which have the rules to trigger --
22 triggered based on exfiltration operations. Patent Owner also argued that the
23 rules could not be enabled on an IPS like Sourcefire, because it would have
24 had too much of an adverse effect. I think the biggest problem with Patent
25 Owner's argument is essentially that it's an argument against the utility of

1 embodiments of the '343 Patent, that two methods disclosed in the '343
2 Patent would more broadly block traffic, equivalently or more broadly block
3 traffic than the rules disclosed in Emerging Threats and Sourcefire. And so,
4 there's no adverse effect that these rules would have that would not be
5 present in the rules of the '343 Patent itself. To the contrary, there's more in
6 the Emerging Threats rules to mitigate blocking, adverse effects of blocking
7 traffic that is desirable. For example, the SSLv3 rule has the prior rules that
8 allow packets to go through using various known ports. And so, you have
9 the flow bits within those prior rules being set saying, you know, if you're
10 using a port for encrypted traffic that's known to be good, then that's not
11 gonna trigger the later SSLv3 rule. And we don't have any mechanisms like
12 that disclosed in the '343 Patent for allowing desirable traffic or legitimate
13 traffic through. Instead, the '343 Patent is just simply, you know, if it has an
14 out-of-date SSL or TLS, block it, or if you're using HTTP, PUT, POST,
15 block it. And so, it's a brighter, more false positives method that was
16 disclosed in Emerging Threats.

17 They also argued, Patent Owner argued, that Dr. Staniford's
18 testimony explained that an IPS owner, or that he didn't explain enabling
19 these rules. And Dr. Staniford's testimony actually explained that an IPS
20 owner would tune the rules to their network environment. And while not
21 every IPS owner might want to turn on all of the rules, Dr. Staniford
22 explained that a user of these rules would load them into the system, could
23 set them to alert, could observe how they work, and then could set them to
24 drop. And so, this was in a 268 demonstrative slide at 268, sorry, Staniford's
25 testimony at 268, which is in our demonstrative slides, explaining this

1 iterative process. So, in a real-world environment, people could test these
2 rules and set them to block.

3 Also, I mean, under *KSR*, this is obvious whether or not these are
4 actually set to block in the field. But here, you have clear teachings of the
5 rules. You have a system that implements these rules and sets them to alert
6 or block. And so, whether or not someone in practice would be regularly
7 using this rule, the combined teachings of these references teach someone
8 that it was desirable to use in your network, you have this rule. So, if your
9 network is a network that might have SSLv3 traffic and you want to block it,
10 then here's a rule you can turn on. Here are all the pieces. It just takes
11 ordinary skill to import this rule and turn it on. It doesn't take an invention.

12 Also, to all of the comments about the large number of false
13 positives, there's no evidence presented by Patent Owner that there would be
14 a large number of false positives with this. SSLv3 was a very out of date
15 encryption protocol back in 2010 at the time of these references prior to the
16 '343 Patent. And so, in a given network environment, they could test this
17 rule, set it up to alert, observe the network traffic, see, you know, there is
18 some traffic using this. It's being -- at risk of being exfiltrated by malware
19 and then set it to block. That would be the normal operation of someone
20 operating an IPS.

21 Patent Owner also argued that we did not analyze whether the
22 Sourcefire reference could itself be modified in the prior challenges and has
23 found that one would not have modified the reference. Here, the challenge
24 again is Sourcefire in combination with Emerging Threats. They also
25 argued that one could load Emerging Threats' rules into Sourcefire, but not

1 that one would. And the record didn't establish that one would. And again,
2 that's wrong. Dr. Staniford repeatedly testified that it was desirable to block
3 exfiltration. And so, that desire shows that while not every IPS owner might
4 turn on all rules, there was a motivation to set the rules for blocking
5 exfiltration's to block. And that was, for example, in paragraph 233 of Dr.
6 Staniford's declaration, which was cited in the petition at 37.

7 JUDGE AMUNDSON: This is Judge Amundson. I had a
8 question. And if you could go to Centripetal's slide 10.

9 MR. DONOVAN: All right. I'm with you.

10 JUDGE AMUNDSON: And it looks like that's your slide. What
11 you're showing on the screen is Keysight's slide. I want to ask about
12 Centripetal's slide. There we go. You got that up on the screen now. And
13 it looks like what they have there is an excerpt from a listserv conversation
14 in 2022 where the people who are using the Emerging Threats rules indicate
15 that they're commented out because they have excessive false positives or
16 performance issues. What's your evidence rebutting that?

17 MR. DONOVAN: All right. Yes. So, Dr. Staniford explained --
18 I'll have to fine the citation. But that the performance issues would be
19 analyzed on any IPS, and you'd be looking when you tune the rules, when
20 you're deciding which ones to enable, it's based on the network environment
21 you have, the processor impact of using these rules or resource impact. And
22 so, you determine which ones to turn on. Here, these rules, because they're
23 both checking for the -- well in this, in at least one of the specific sets, the
24 legitimate higher level ports and then checking for the packets that are using
25 the old version of SSL or TLS. Those are more resource intensive, and they

1 have some false positives. And so, in a given network environment you'd
2 want to test that before enabling it. But it's still, this is just the exercise of
3 one of skill in the art, implementing the teachings that are here. The rules
4 are still included in Emerging Threats and distributed so that people with
5 IDSs and IPSs can load these, enable them, test them, and use them if it's
6 appropriate for their environment. And so, these aren't rules that weren't
7 distributed in Emerging Threats, because they are known to have problems.
8 Instead, this is a document that was teaching people, these are known rules.
9 These are rules that can accomplish things. It's up to you to implement them
10 in your environment or not. And that also goes to, I think, a central issue in
11 Patent Owner's arguments that essentially they're arguing against the bodily
12 incorporation of these Emerging Threats rules in a source buyer system and
13 saying it wouldn't be desirable to implement this system in a real world
14 network. And that's not the analysis we're performing here. We're looking
15 at, under *KSR*, under the *Graham* factors, is this obvious? And we have the
16 source buyer reference that teaches that it was known to look to third party
17 rule providers, which Emerging Threats was the largest rule provider of
18 Snort Rules at the time, to see what rules are out there. What you could do
19 to prevent, you know, malicious traffic attacks. And the Emerging Threats
20 reference teaches that it was known to write rules to prevent exfiltration.
21 There's a lot of different ways of doing that. And the combined teachings
22 within Emerging Threats, there are comments explaining for commented out
23 rules. If you want to enable this rule, or if you want to use this rule, enable
24 it. So that's teaching a skilled artisan reading the Emerging Threats
25 reference, here's a rule for you to consider. If you want to enable it, all you

1 do is turn it on. And then you load it into Emerging Threats and you --
2 sorry, into Sourcefire and use it. So, the combined teachings rendered
3 obvious.

4 JUDGE AMUNDSON: All right. Thank you.

5 MR. DONOVAN: Patent Owner also asserted that Emerging
6 Threats is an IDS or intrusion detection system rule provider, rather than an
7 IPS or intrusion prevention system rule provider. Even if, I don't know if
8 that has any merit, but even if it does, Sourcefire teaches expressly loading
9 text rules from third party store providers. And Emerging Threats was the
10 largest third party store provider at the time. So, whatever the intention for
11 creating the Emerging Threats rules were, it's clearly that the combined
12 teachings of the Sourcefire and Emerging Threats teach loading text rule
13 files like this into intrusion prevention systems like Sourcefire that can then
14 set these rules to block traffic.

15 Patent Owner also argued that the '343 Patent is inventive because
16 it has a first cut of checking the IP packet header information or the F-
17 TUPLE information. And they argued that our arguments are ignoring the
18 packet header data. First off, that's not the focus here because the '552 IPR
19 already established that Sourcefire teaches checking that 5-TUPLE
20 information and that first check before we look to the application header
21 information for checking whether or not you have an exfiltration operation.
22 However, even if we were to look at the Emerging Threats rules in the
23 context of the TCP IP header, it's still doing the same thing as the '343 Patent
24 and an improvement upon it. And so, here in the '343 Patent you have
25 essentially Figure 1 is the network environments and you have multiple

1 networks that the packet can be sent between. And then in Figure 3, where
2 you have the chart that has the F-TUPLE checks prior to the operator that
3 can include and require TLS or the HTTP-EXFIL, you're looking at source
4 IP addresses and destination IP addresses inside or outside of these networks
5 to know which packets you're going to be looking at the application header
6 information on, and which you're determining whether to allow or block
7 based only on the F-TUPLE information. And that's the same thing that you
8 see in the Emerging Threats rules. And so, and this is part of Snort Rules in
9 general, but the SSLv3 rule we look at, that has, and that's in Emerging
10 Threats at page 109. It has the first part of the rule is this 5-TUPLE check.
11 You're checking if it's from the home net at any port to an external net at a
12 port range. And so, just like the '553, sorry the '343 Patent, you have this
13 limitation as to the ports and IPs that are being checked. And it would just
14 be ordinary skill in the art to further refine that and anyone implementing
15 this rule would determine what packets they want to apply this against. It
16 doesn't necessarily have to be against all traffic. That's just normal operation
17 of an IPS or IDS to configure the rules.

18 They also argued that there's no evidence that Keysight tried to
19 implement their rules on an IDS and that it worked. This is an IPR in the
20 prior art issue. Here are the documents and their teachings, not the bodily
21 incorporation of the Emerging Threats rules into an IPS.

22 Patent Owner also argued that there was no dispute about Mr.
23 Marinho's testimony where he was saying that someone wouldn't load these
24 rules into an IPS and set them to block. However, Mr. Marinho admitted in
25 his deposition that he had no experience, not at all in the context of

1 managing an intrusion prevention system, and that's in the reply at page 12
2 which cites to Mr. Marinho's deposition which is Exhibit 1101 at 28 and 29.
3 So, while Mr. Marinho is saying that someone operating an IPS would not
4 go and set these rules to block, he has no experience operating an IPS. He
5 doesn't know if someone operating an IPS, he doesn't have the qualifications
6 to opine about what someone operating an IPS would do.

7 Dr. Goodrich, similarly, he opined that someone wouldn't enable
8 these. He testified in his deposition that he had no experience with Snort
9 Rules at all until his retention by Patent Owner sometime in 2016. And that
10 was in the reply at 12, citing Exhibit 1100 at 13 to 15.

11 All right. Patent Owner's counsel also argued that read in context,
12 this rule is not about SSLv3, it's about other versions of SSL and TLS. I
13 don't see that support in Exhibit 1020 itself. Specifically, there are only two
14 rules in this portion of the rule set that check for versions of SSL or TLS.
15 The one we cite to on page 109 is Exhibit 1020. It's three up from the
16 bottom. That's the SSLv3 rule. The one immediately before that checks for
17 content 170301 in the application header. And in our petition, we cite to the
18 TLS reference documents, and that explains that that header value is for
19 checking the TLS 1.0. So, the only rules we have here are ones that are
20 checking for TLS 1.0 or SSL version 3. These are both versions of the SSL
21 TLS protocol that were long out of date by 2010.

22 Patent Owner also argued that the uniform resource identifier is not
23 identifying a resource. By definition, a uniform resource identifier is
24 identifying a resource. Patent Owner also argued that in my arguments, I
25 was identifying the resource as the 5-TUPLE Data, and Patent Owner was

1 saying that it, the specification referred, well either way, to clarify my
2 argument, Patent Owner asserts that the specifications reference to resource,
3 as I understood it, was referring to the 5-TUPLE Data. That is not what's
4 being checked in the application header where it's checking the resource in
5 claims 5 and 12.

6 JUDGE TURNER: Counsel, you have two minutes.

7 MR. DONOVAN: Thank you. As to the waiver issue, I'll just
8 note that Patent Owner did not make any arguments that its resource
9 argument for claims 5 and 12, or that resource is not disclosed by a uniform
10 resource identifier were made in the Patent Owner's response.

11 And just as a last point regarding c availability, Patent Owner
12 argued that there are 11,000 rules within Emerging Threats and that
13 someone wouldn't know that this specific rule was for exfiltration.
14 However, the record establishes that Emerging Threats themselves were a
15 prior art reference. And so, someone would look for Emerging Threats if
16 they were looking for sources of Snort Rules which show, you know, the
17 capabilities within the cybersecurity space for blocking traffic for various
18 reasons. And a hypothetical person of ordinary skill in the art would be
19 presumed to know the contents of the references that were available. And
20 this is certainly a reference that was -- was well known at the time.

21 And unless the Board has any questions. All right. Thank you.

22 JUDGE TURNER: Thank you, Mr. Donovan. I will move back to
23 Mr. Price for sur-rebuttal. Counsel, you have six minutes. You may begin
24 when you're ready.

25 MR. PRICE: Thank you, Your Honor. You can launch. Can you

1 see the demonstratives again? Okay. Judge Amundson, thank you for your
2 focus on here, because this really gets to the crux of the case. These IDS
3 rules are written for IDS devices. Mr. Marinho, he said he doesn't have any
4 experience with IPS devices because he wrote IDS rules. He wrote, and this
5 is at the time of the invention, I should say, he wrote IDS rules. And the
6 idea that any person would have put one of these rules on to block live
7 traffic, horrifying. There is undisputed testimony from a person who wrote
8 many of the rules in Emerging Threats that these rules were not what they
9 were made -- this is not what they were made for. And a person of ordinary
10 skill in the art wouldn't have done it. And what do we not have actually in
11 the record? Any evidence that a person of ordinary skill in the art would
12 have done what Petitioner says that you would do with these. My opposing
13 counsel, you know, again, said, well, you could put them in, we'll use them
14 as alert rules and then decide whether or not one of them, you know, could
15 be turned to a drop rule.

16 However, they didn't do that with any of these rules and, you
17 know, this is about reasonable expectation of success with a modification
18 that they need of the prior art to reach the challenged Claims. They have not
19 demonstrated that reasonable expectation of success because if you had
20 turned on any of these rules with false positives, with poor performance, you
21 would have broken the system. The system would not have worked. You
22 could not have run your network using these rules. They were not designed
23 for that purpose. And a person of ordinary skill in the art would not have
24 turned them on, and there is no evidence in the record that any person of
25 ordinary skill in the art would have implemented any of the identified rules.

1 It's missing from the record.

2 Now, my friend, you know, said during his rebuttal -- sur-rebuttal
3 was that well, you know, you could kind of see how they run. But they
4 didn't do that. They -- he also said that this is about bodily -- our argument
5 is about bodily incorporation. It's not about bodily incorporation. It's about
6 whether or not a person of ordinary skill in the art would have modified the
7 prior art teachings to reach the claimed invention. Our argument, you know,
8 from the beginning, is that a person of ordinary skill in the art would not
9 have turned any of these alert rules into drop rules for reasons that are
10 undisputed in the record. It will -- poor performance, too many false
11 positives would make the device unusable in your network. No person of
12 ordinary skill in the art would have modified the rules as suggested.

13 I heard that SSLv3 was considered, you know, well past its time by
14 the time of the invention. If you look at an Exhibit 1100 from 23.1 to 24.4,
15 it's SSLv3 was still being used 2014, 2015, 2016. So, there were known
16 vulnerabilities in SSLv3, however, it was still used widely up until at least
17 2016. But we also didn't hear any answer to the fact that these rules about
18 SSL and TLS on high ports are not just looking for outdated protocols,
19 outdated encryption protocols. Every version of the protocols were included
20 here because all they're looking for is encrypted traffic on the high port
21 because that's the signature of this particular (INDISCERNIBLE). And this
22 is not a rule that was designed to prevent an exfiltration operation because
23 one of these SSL versions was out of date.

24 JUDGE TURNER: Counsel, you have two minutes.

25 MR. PRICE: Thank you. Again, you know whether or not, you

1 know, I think my friend's main argument is that, well, it would have been
2 desirable to present exfiltration's, right? If you had a rule that, you know,
3 could potentially block exfiltration's, why not just turn it on? But, you
4 know, I think the record is clear that if you had done that with any of these
5 rules, you would have ended up with a broken system and an unused
6 (INDISCERNIBLE). So, with that, and unless there are any questions,
7 thank you for your time.

8 JUDGE TURNER: Thank you. The case is submitted. We'll go
9 off the record.

10 (Whereupon the above-entitled matter went off the record at 2:37
11 p.m.)

IPR2023-00446
Patent 10,567,343

PETITIONER:

Gerard M. Donovan
Peter J. Chassman
Walter M. Egbert
Jonathan I. Detrixhe
Sidharth Kapoor
REED SMITH, LLP
gdonovan@reedsmith.com
pchassman@reedsmith.com
WEgbert@reedsmith.com
jdetrixhe@reedsmith.com
skapoor@reedsmith.com

James L. Davis, Jr.
ROPES & GRAY LLP
james.l.davis@ropesgray.com

PATENT OWNER:

James Hannah
Jeffrey H. Price
Jenna Fuller
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com
svdocketing@kramerlevin.com

Bradley Wright
Scott M. Kelly
John. R. Hutchins
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
jhutchins@bannerwitcoff.com