

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GEOSECURE, INC.,
Patent Owner

IPR2025-00070
Patent 9,954,872 B2

Record of Oral Hearing
Held: June 10, 2026

BEFORE: STACEY G. WHITE, NEIL T. POWELL, and
GARTH D. BAER, Administrative Patent Judges.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

PAUL HART, ESQ.
STEN LARSON, ESQ.
Erise IP
7015 College Blvd #700
Overland Park, KS 66211
(913) 777-5600
paul.hart@eriseIP.com
sten.larson@eriseIP.com

BENJAMIN HUH, ESQ.
CrowdStrike, Inc.

ON BEHALF OF THE PATENT OWNER:

GIRI PATHMANABAN, ESQ.
STEVEN W. PETERS, ESQ.
DAVID HLAVKA, ESQ.
Cleary Gottlieb Steen & Hamilton LLP
2112 Pennsylvania Ave NW
Washington, D.C. 20037
(202) 974-1500
gpathmanaban@cgsh.com
speters@cgsh.com
dhlavka@cgsh.com

JACOB LEVINE, ESQ.
GeoSecure, Inc.

The above-entitled matter came on for hearing on June 10, 2026,
commencing at 1:00 p.m., via video teleconference.

1 P R O C E E D I N G S

2 - - - - -

3 JUDGE POWELL: Welcome. Please sit. Good
4 afternoon. This is the hearing for IPR 2025-0070. The challenged
5 patent for that matter is US Patent No. 9,954,872 B2. I am Judge
6 Powell, joined by Judges Baer and Judge White. Who do we have
7 attending for Petitioner today?

8 MR. HART: Good afternoon, Your Honor. Paul Hart
9 with Erise IP for Petitioner. With me today is Sten Larson, also
10 from Erise IP, and Benjamin Huh, in-house counsel for Petitioner.

11 JUDGE POWELL: Thank you. And who do we have
12 attending for Patent Owner today?

13 MR. PATHMANABAN: Good afternoon, Your Honor.
14 This is Giri Pathmanaban with Cleary Gottlieb for Patent Owner
15 GoSecure. With me today is my colleague, Steve Peters. We will
16 share argument between me and Steve today, and we also have our
17 colleagues, David Hlavka and Jacob Levine.

18 JUDGE POWELL: Very good. Per our hearing order,
19 each side will have 60 minutes to argue. Petitioner will begin and
20 may reserve rebuttal time for response. Patent Owner will respond
21 to Petitioner's case in chief and may reserve time for surrebuttal.
22 I'm going to keep track of each party's time on this timer behind
23 me. I hope to let you know when you're getting close to the end,
24 but please try to keep track of your time also. When you present,
25 please let us know orally which demonstratives, exhibits, papers,

1 that sort of thing that you're referring to. It's good for the
2 transcript, and it helps Judge White, who is not here in the
3 courtroom. I think with that, we're just about ready to go. Does
4 Patent Owner have any questions before we start?

5 MR. PATHMANABAN: No, Your Honor.

6 JUDGE POWELL: Anything from Petitioner?

7 MR. HART: No, Your Honor. Other than courtesy
8 copies of our slides, I can bring those up if they'd be helpful.

9 JUDGE POWELL: Yeah, sure. We'll take a copy. How
10 much time would Petitioner like to reserve, if any?

11 MR. HART: We'll reserve 15 minutes for rebuttal, Your
12 Honor.

13 JUDGE POWELL: Okay. I'm going to change the timer
14 to reflect the 45 minutes, so you don't panic and think you're
15 running out of your hour. Ready?

16 MR. HART: I am ready. Thank you.

17 JUDGE POWELL: We are ready. Thank you.

18 MR. HART: All right. Very good. This case is largely
19 about GoSecure's improper attempt to recapture matter dedicated
20 to the public in a prior patent application publication. In 2007,
21 nearly three years before the priority date for the challenged patent
22 here, GoSecure's predecessor filed a patent application that issued
23 as Capalik, the primary reference in every ground that we are
24 going to discuss here in today's proceeding. It is undisputed that
25 Capalik is 102(b) prior art. It is also largely undisputed that

1 Capalik and the '872 Patent describe starkly similar systems,
2 architectures, functionalities, using nearly verbatim language in
3 many relevant respects. Throughout this proceeding, GoSecure
4 has attempted to distract from the similarities between Capalik and
5 the '872 Patent by mischaracterizing the intrinsic record in two
6 specific ways. First, GoSecure asked the Board to ignore express
7 teachings and express embodiments in the '872 Patent, excluding
8 them from the claims as a way to distinguish its claim scope from
9 Capalik's disclosures. Second, GoSecure manufactures disclosures
10 ascribing them to the '872 Patent and then criticizes Capalik for
11 failing to capture those imagined details. For GoSecure's
12 ignore-the-inconvenient-embodiments approach, it asked this
13 Board to construe computer system such that it captures only
14 individual protected endpoint devices. Now, this is a position that
15 seeks to exclude from the claims express embodiment in the '872
16 Patent, where attack information is sent to a protected network,
17 including the IDS, IPS of that protected network. This
18 embodiment happens to align precisely with an embodiment
19 described in Capalik, the prior art. In addition to excluding an
20 express embodiment via this argument, GoSecure's request that the
21 Board construe the claims in that way also ignores two out of three
22 express meanings that the '872 Patent ascribes to the term
23 computer system. Now, at institution, the Board correctly rejected
24 this narrow interpretation of the claims, finding the record did not
25 support construing computer system to exclude all of that express

1 disclosure in the '872 Patent. The fully developed record provides
2 the Board no reason to deviate from that correct preliminary
3 finding. Turning to GoSecure's imagined disclosure approach, it
4 takes aim at the claimed data structure. Now, there's no dispute in
5 this record that both Capalik and the '872 Patent teach
6 introspection modules that monitor attacks as they occur on a
7 virtual machine in a decoy device that generates forensic data of
8 the attacks, and it uses that forensic data to generate a fingerprint
9 that is sent off to another computer system, so that other computer
10 system can avoid damage due to similar attacks. Seeking to create
11 delta between Capalik and the '872 Patent where none exists,
12 GoSecure argues that the claimed data structure is something
13 different than forensic data, something beyond what forensic data
14 provides by itself. It points to the charts, the data arrangements
15 depicted in figures 5A and 5B in the '872 Patent, and it stresses
16 that Capalik fails to include similar figures in its disclosure. Now,
17 when I cross-examined GoSecure's expert, he conceded that the
18 patent does not explain what the difference is between the forensic
19 data and those charts, the arrangements of data in those figures.
20 The reason is the claimed data is the forensic data. The claimed
21 data structure in limitation 1C is the forensic data, and the
22 disclosure of creating and using that forensic data is identical in
23 Capalik and the '872 Patent.

24 JUDGE BAER: Counsel, is there anything to data
25 structure that's different from data, or are they just entirely the

1 same?

2 MR. HART: The claims recite a data structure. They
3 expressly define what data needs to be contained in that data
4 structure, and that's in Claim 1. Claim 3 comes in and explains
5 how that data is used. And specifically, Claim 3 recites creating a
6 fingerprint from that stored data structure.

7 JUDGE BAER: But in the interest of giving structure
8 some sort of value beyond data, is it your position that there's no
9 distinction between data and data structure such that all data would
10 be structured data, or is there some delta between the two?

11 MR. HART: Our position is that all useful data that is
12 used in the way the patents describe is stored with some useful
13 structure so that that data can be used. So --

14 JUDGE BAER: So would usefulness be the distinction
15 you're drawing?

16 MR. HART: That's certainly what our expert explained
17 in his opening supporting declaration that it was well known to
18 store data in systems like this in a way where you can extract
19 useful information. If you're storing activity sources, targets and
20 their associations so that you can use that information to generate a
21 fingerprint, which is exactly what Capalik and the '872 Patent
22 teach, they need to be stored in a structure that allows that
23 information to be used, to be extracted into a fingerprint that can
24 be sent on to the protected computer network in this specific
25 context.

1 JUDGE BAER: And you keep addressing what is
2 structured data, and I appreciate that. Can you give me an
3 example, and perhaps the only example is useless data, but can you
4 give me an example of what is not structured data? What is data
5 but is not structured data?

6 MR. HART: Sure. I don't -- we don't have any examples
7 of unstructured data in the record that I can point you to. But
8 certainly the highlight from our expert explaining what this means
9 based on the intrinsic record is usefulness. And there are examples
10 in the supporting expert declaration, Exhibit 1003, of structured
11 data as it was well known in the art. And again, it's
12 -- Bhattacharya is a secondary reference that he pointed to with a
13 figure of how that data is structured and stored so that it can be
14 usefully extracted to be used.

15 JUDGE BAER: Thank you. That's helpful.

16 MR. HART: Turning to slide --

17 JUDGE WHITE: Counsel?

18 MR. HART: Yes, Your Honor.

19 JUDGE WHITE: On that same point, would you
20 concede that the term data structure is a well-known term in the
21 art?

22 MR. HART: Yes, Your Honor. That is certainly
23 something that Dr. Jacobson, Petitioner's expert, addressed in his
24 opening declaration, Exhibit 1003. He explained that data
25 structures are well known in computer science and specifically the

1 point I was alluding to earlier, that they are necessary in order to
2 store data to be used in a useful way. So there must be a data
3 structure. The phrase data structure was well known and by itself
4 does not impose any particular arrangement of the data beyond
5 simply allowing that data to be used as desired.

6 JUDGE WHITE: But wouldn't you say that the term
7 data structure requires there to be some particular arrangement?
8 Not necessarily one particular specified arrangement because I
9 don't see in the claims that they have a specific data structure, but
10 there has to be some sort of a structure in place, whether that be an
11 array, a tree, a grid, something. Would you agree that there's some
12 structure?

13 MR. HART: Yes. We agree that there must be some
14 structure, and that is where using that data comes into play. So in
15 both Capalik and the '872 Patent, that forensic data is stored in a
16 way that allows a fingerprint to be created from that stored data.
17 So there is a structure necessarily of that stored forensic data
18 because a fingerprint that is useful by other systems is extracted
19 from that data and transmitted to the protected computer network.
20 So it is simply requiring some useful structure so the data can be
21 used. It does not specify what that arrangement is. It does not
22 exclude any particular arrangements of data beyond, I suppose,
23 random storage of data from which useful information could not be
24 extracted.

25 JUDGE WHITE: So going with what you're saying that

1 there is a broad understanding of the range of data structures that
2 are available, what data structure is there in Capalik that you are
3 pointing to as far as a structure?

4 MR. HART: Sure. There is no specific illustrated
5 example of how that data is stored. There is express disclosure of
6 using that stored data to generate a fingerprint that is sent from the
7 decoy network to the protected network. So we have the express
8 teaching that that data has been stored in a useful structure so that
9 the fingerprint can be extracted and sent onto a protected network
10 in order to ensure similar damage is not caused in that protected
11 network.

12 JUDGE WHITE: Isn't Capalik stored in a particular
13 relational database, though? Does that not have a structural
14 requirement to it?

15 MR. HART: It --

16 JUDGE WHITE: It's a relational database.

17 MR. HART: -- it absolutely does, Your Honor. And
18 when I say there is no description or illustration of exactly how
19 those data fields are laid out, they are laid out in that relational
20 database per the requirements of that relational database, and we
21 know that they're structured because they are then used to generate
22 a fingerprint. So yes, you're exactly right. That relational database
23 does provide some mandatory structure. We just -- because these
24 concepts are so well known, Capalik itself doesn't go into the
25 details of showing us how that data is laid out one data point with

1 respect to another data point.

2 JUDGE WHITE: So are you saying by virtue of the fact
3 that it is in a relational database, it is a data structure?

4 MR. HART: That is --

5 JUDGE WHITE: Is that --

6 MR. HART: Yes, Your Honor. That is one reason it is a
7 data structure, but not the only reason it is a data structure. I think
8 a very important additional reason is this additional teaching in
9 Capalik that is identical in the '872 Patent, that that forensic data is
10 stored such that a fingerprint can be generated from it to be sent on
11 to the protected network. So it's not just that we're storing it in a
12 relational database, it's that we're storing it in a relational database,
13 providing structure, and that structure allows us to extract what
14 matters out of the stored forensic data in order to send that
15 information on to the network. You are all obviously very up to
16 speed, so I will breeze through some of these early slides here.
17 The '872 Patent's disclosure: the basic concept is you have a decoy
18 device running one or more virtual machines. Those virtual
19 machines are less susceptible to attacks from networks. Those
20 attacks are allowed to come in and run on the virtual machines,
21 and they are monitored by an introspection module. The
22 introspection module generates forensic data, and that forensic
23 data is stored and then used to generate a fingerprint that could be
24 sent off to a protected computer network to make sure other
25 devices on that protected computer network are not susceptible to

1 harm from similar attacks. Illustrative claims. Claim 1 walks
2 through the general structure of these methods that are described in
3 claim in the '872. We have monitoring on a first computer or first
4 computer system, excuse me, storing that data structure that we've
5 been discussing, and then transmitting attack information onto a
6 second or other computer system. Claim 3 is relevant to some of
7 the issues the parties are disputing. That recites creating from the
8 stored information, so from the stored data structure that we've
9 been discussing, a fingerprint indicative of the attack activity that
10 occurred on that first computer system. As I alluded to in my
11 opening remarks, Capalik and the '872 Patent are remarkably
12 similar. They share an inventor. They describe the same
13 architecture, the same functionalities. They both utilize decoy
14 networks with decoy devices running one or more virtual
15 machines. Those virtual machines attract and monitor attacks.
16 They generate forensic data of the attacks. From that forensic
17 data, they generate signatures or fingerprints and then transmit
18 those onto other computer systems to make sure other devices are
19 not susceptible to harm from similar attacks. They each disclose
20 protected networks that receive those signatures or fingerprints.
21 And in each Capalik and the '872 patent, the protected network
22 includes an IDS, IPS, an intrusion detection or intrusion prevention
23 system, as well as multiple protected endpoint devices. Here are
24 the architectures from figure 1 in the '872 and figure 5 from
25 Capalik. In both, I have annotated red, the decoy network. Here

1 we see that in each case, they rely --

2 JUDGE POWELL: Sorry to interrupt you. Just not to
3 nag, you're on Slide 5, right?

4 MR. HART: Thank you, Your Honor. If you --

5 JUDGE POWELL: We appreciate the pace because we
6 want to keep going, but --

7 MR. HART: I understand. Every transcript I've ever
8 read, I wish I had done more to forecast where I was referring to.
9 DX 5 is what we're looking at right now. DX 5 includes figure 1
10 from the '872 Patent, figure 5 from Capalik. In both, in red, we
11 have a decoy network comprising a decoy device. Those are the
12 devices less susceptible to attacks, so those attacks can be
13 monitored. And in each case, we have in blue a protected
14 computer network comprising IDS, IPS, as well as multiple
15 protected network devices.

16 DX 6 summarizes the grounds. As I mentioned earlier,
17 each depends on Capalik primarily. King, Pike and Farley are
18 brought in grounds 3, 4 and 5 for dependent claim concepts. Goel
19 is introduced in ground 2 as well as in the alternative in grounds 3
20 through 5 to provide an express teaching of pulling from
21 monitored data, activity sources, targets, and associations. That
22 was presented to account for the possibility that Patent Owner
23 would argue the forensic data described in Capalik does not
24 include those three data points. It does not appear on that record
25 they are taking that position. It appears to be conceded that the

1 forensic data in both the '872 Patent and in Capalik include all
2 three of activity sources, targets, and associations. DX 7
3 summarizes the remaining independent claim disputes, which I
4 will skip for now because I will cover them each in detail. DX 7
5 summarizes which dependent claims have remaining disputes
6 between the parties. I'll handle that one similarly. So DX 9 brings
7 us to computer systems. Now, this is the only substantive dispute
8 that was raised pre-institution. This relates to the meaning of
9 computer system.

10 As we see here in claim 1, claim 1 recites monitoring
11 activity on a first computer system, transmitting activity
12 information to one or more computer systems other than the first
13 computer system. So we -- I'll refer to them as a first computer
14 system and a second computer system for simplicity today. In
15 both Capalik and in the '872 Patent, the information is sent from
16 the decoy network and the decoy device to a protected computer
17 network. In both Capalik and in the '872 Patent, that protected
18 computer network includes an IDS, IPS, as well as multiple
19 protected endpoint devices. Now, in the '872 Patent, some
20 embodiments, the IDS, IPS receives that fingerprint, and in some
21 embodiments, the endpoints receive that fingerprint -- so the
22 information about the attack from the decoy device. The question
23 for the board is whether the claim language should be construed to
24 exclude the express embodiments where the IDS, IPS receives that
25 fingerprint or signature of the attack. And that largely boils down

1 to the meaning of computer system. How should computer system
2 be construed in this case? And that will answer the question as to
3 whether some express embodiments are captured or excluded from
4 this claim. GoSecure argues that computer system should be
5 construed to be limited to a single endpoint device, protected
6 endpoint device, and that the claims require transmitting
7 fingerprints to those endpoint devices and exclude the express
8 embodiments where the IDS, IPS receives a fingerprint.
9 Petitioner's position is that computer system is more broadly
10 treated by the intrinsic record and that it should not be so limited,
11 that it should capture sending those fingerprints to any component
12 within that protected computer system that contains the IDS, the
13 IPS, and those protected devices.

14 Now, very briefly, DX 10, before I get into the substance
15 of the claim construction dispute, there is a challenge that our
16 petition did not clearly identify the protected network as the
17 recipient of that fingerprint. As I have here, just some examples
18 from the petition and supporting expert declaration, we did identify
19 protected network 504 as the recipient of that fingerprint. Both the
20 petition at -- there's actually quite a bit of discussion at petition
21 page 33. Here we have a quote from petition page 34 and a
22 lengthy discussion from our expert declaration, including
23 paragraph 143. As you'll recall, there was some post-petition
24 briefing or post-POPR briefing here related to this issue. And as
25 the board explained in its institution decision at 12, it

1 acknowledged that our position was that the information about the
2 attack is transmitted to the protected network, which includes
3 protected endpoint devices and the IDS, IPS. So at the very least,
4 as of institution, everybody was on notice that this is the theory
5 being pursued here along with the evidence that this was in fact the
6 theory that was presented in our petition as well as our supporting
7 expert declaration. DX 11 gets to the intrinsic record. What does
8 the intrinsic record say with respect to computer system? Well, it
9 treats that phrase very broadly. It provides multiple different uses
10 and meanings of that phrase, including referring to subcomponents
11 of a computing device, such as the virtual machine. So that is a
12 sub module within a larger computing device. It does use
13 computer system to refer to whole computing devices themselves,
14 and it also uses computer system to refer to collections of devices.
15 So here in figure 1, a figure the board pointed to and discussed in
16 its institution decision, we see multiple devices connected via
17 network connections. Those are also treated as a distributed
18 computer system. So we have narrow use referring to
19 subcomponents, middle use referring to a device standing alone,
20 and also collections of computing devices all being referred to as a
21 computer system. Now, GoSecure takes the position that the
22 narrow use, the subcomponent, that, yes, it acknowledges the
23 patent defined that as a computer system, but it says the patent
24 didn't really mean that. It says the broader use that captures a
25 network of computers is too broad and the patent didn't really

1 mean that. And they ask you to take sort of the Goldilocks
2 approach to claim construction and choose only one of those three,
3 and that is the lynchpin of this entire argument. You excluding
4 two out of the three uses of computer system in the intrinsic record
5 and limiting these claims to only one of those three. If you do not
6 do that, this argument falls from that matter.

7 JUDGE POWELL: Does Petitioner argue that the
8 embodiment, the disclosed embodiment in the '872 Patent
9 involving transmission to the -- of the fingerprint just to the
10 IDS/IPS, does the spec ever use the word computer system when
11 talking about that specific embodiment?

12 MR. HART: I can certainly have my colleague look and
13 come back. Off the top of my head, I'm not aware of an instance
14 in which the IDS/IPS as part of the protected computer system is
15 itself referred to as a computer system.

16 JUDGE POWELL: Or anything in that embodiment. I
17 think part of the Patent Owner's argument is when the specification
18 describes that embodiment, it never really uses computer system to
19 refer to any component in there. Is that --

20 MR. HART: That is certainly -- well, or all of the
21 embodiments, right? So there is certainly a collection of devices,
22 including the IPS, IDS, and the endpoint devices that are part of
23 that protected --

24 JUDGE POWELL: Right.

25 MR. HART: -- computer system network. The patent

1 certainly uses computer system to refer to collections of devices as
2 well as individual devices and subcomponents. And so does the
3 patent tie the phrase computer system specifically to one of the
4 embodiments of sending the signatures? I don't believe so. But I
5 think the same is true of the endpoint devices.

6 JUDGE POWELL: Okay. Thank you.

7 MR. HART: In DX 12, the similarities in the
8 architectures between Capalik and the '872, which I've already
9 covered to some extent, also support Petitioner's position that it is
10 improper to read out these express embodiments. As I've covered
11 in both Capalik and the '872, the decoy network monitors attacks,
12 creates forensic data, generates fingerprints from that forensic data,
13 and sends that off to the protected network on DX 12, which is
14 annotated blue. In both Capalik and the '872 Patent, the protected
15 computer networks in blue contain both an IDS, IPS, as well as
16 multiple endpoint devices. And both Capalik and the '872 describe
17 embodiments that perfectly align where those fingerprints are sent,
18 not just to the protected network, but to the IDS, IPS specifically.
19 GoSecure insists --

20 JUDGE WHITE: Can I ask you to address one of the
21 Patent Owner's arguments specifically? And that's that the
22 language of Claim 1 would render this sort of a construction
23 meaningless. The language of Claim 1 where it says that a
24 computer system is attached to a computer network. And they say
25 that the way that you're reading computer system would make that,

1 basically, computer system is attached to a computer system.

2 MR. HART: Yes.

3 JUDGE WHITE: That they're not a meaningful
4 limitation.

5 MR. HART: Absolutely, Your Honor. So focusing on
6 the right side of DX 12, this is figure 5 from Capalik. We see
7 attack activity -- sorry about that. Attack activity in a circle
8 labeled 550. And I may or may not be able to zoom in here. This
9 is the connection to the network that we have pointed to in the
10 claims. This is where those network-based attacks come into the
11 virtual machine in order to attack the virtual machine and be
12 monitored so that those fingerprints can be generated. This is
13 separate from the protected network. This is separate from the
14 decoy network. It is an entirely separate network in the -- in
15 Capalik functionally. The argument that, as I understand their
16 argument, it essentially tries to say that if computer system is so
17 broad that it captures network computers, then it captures
18 everything on Earth, and there's no way to define computer system
19 as everything on Earth and make it make sense here. That extreme
20 case is certainly not our position. Our position that computer
21 system based on the intrinsic record is not limited to one device,
22 but can be a collection of devices. It's not a binary between one
23 and everything. It's a binary between one and one or more. So
24 that is the heart of their argument with respect to the network.
25 There is no inconsistency in our mapping.

1 JUDGE POWELL: So, okay, so on Judge White's point,
2 and I think what you're saying is that their argument doesn't
3 address the way you've mapped the --

4 MR. HART: That's exactly right.

5 JUDGE POWELL: -- prior art to the claim.

6 MR. HART: It doesn't address the way we've mapped it,
7 and it certainly doesn't address the way we've addressed the claim
8 construction of computer system, right? It almost ascribes the
9 most extreme possible example of computer system as literally
10 every device in the world and claims that that is our position,
11 which it is certainly not.

12 JUDGE POWELL: How -- pardon me. How concerned
13 should we be that about the -- about Patent Owner's argument that
14 the term would be boundless if we don't limit it to something more
15 specific, I guess, is --

16 MR. HART: Well, I think the structure of the claim
17 prevents that, right? The structure of the claim identifies one or
18 more computer systems other than the first computer systems. So
19 it's already placing bounds, right? There's already the possibility
20 of at least multiple other computer systems that receive this
21 fingerprint in order to protect themselves from similar attacks. So
22 the structure of the claims does not allow this to be a boundless,
23 nor is there support in the intrinsic record for construing that as a
24 boundless, every computer device that's connected on Earth. And
25 we certainly have not suggested that interpretation of computer

1 system.

2 I will say on this point before leaving DX 12, the entire
3 argument essentially from Patent Owner is the patentee intended to
4 exclude express embodiments and the -- that we know the patentee
5 intended that because they used the phrase computer system. That
6 all comes back to the interpretation of computer system. Now,
7 there are certainly endpoint devices described in the '872 Patent. If
8 they intended to limit these claims to an endpoint device and
9 exclude the embodiments that are expressed, where that fingerprint
10 is sent to an IDS, IPS, they certainly could have drafted the claims
11 to require transmitting that information to an endpoint device.
12 They did not. GoSecure, Patent Owner in this case, has not moved
13 to amend these claims, and so the claims exist as they stand. They
14 recite computer system, and that phrase is used far more broadly
15 than Patent Owner would like it to be -- to be limited to individual
16 endpoint devices in isolation. Jumping to DX 14, I'm going to
17 pick up the next major dispute between the parties that touches on
18 the independent claims, and this relates to the data structure
19 dispute.

20 As I have here on DX 14, language from Claims 1C and
21 Claim 3. These -- this is the primary claim language implicated by
22 the data structure fight. So Claim C recites storing in the memory
23 a data structure that identifies the activity sources, targets, and
24 activities. And then Claim 3 comes in and says, creating from that
25 data a fingerprint indicative of the activity that ran on that first

1 computer system. As we established in the petition, both Capalik
2 and the '872 Patent describe introspection modules that monitor
3 these attacks, that generate forensic data of the attacks, and that
4 use that forensic data to create fingerprints indicative of those
5 attack activities. That teaching is nearly verbatim, materially
6 identical in both Capalik and the '872 Patent. This detailed
7 forensic data includes activity sources, activity targets, and their
8 associations. It is the data that is used to create the fingerprints.
9 This is the data structure. Now, GoSecure, as far as I can tell from
10 this record, does not dispute that those expressly recited data
11 points are included in the forensic data created, and so they have
12 taken aim at an arrangement. They are suggesting that the claims
13 by using data structure require some arrangement. They point to
14 figures 5A, 5B in the '872 Patent and say, this is an arrangement.
15 This is not in Capalik; therefore, Capalik falls outside the scope of
16 the claims. It stops short of arguing that Claims 5A and 5B limit
17 the claims. And this is very important. There is no argument as to
18 what specific arrangement is required by the claims.

19 This is just an argument that the '872 has these figures,
20 Capalik does not; therefore, you should let these claims survive.
21 But as I will walk through, the record reveals there is no
22 meaningful distinction between the forensic data generated in both
23 Capalik and the '872 Patent and the claimed data structure.

24 The first stop I want to make in the record is how -- I'm
25 sorry, I'm going to make this full screen again so I'm not revealing

1 any mental illness from how many thumbnails I have on my
2 desktop -- this is a slide that addresses DX 15, how GoSecure
3 treated the claimed data structure when it came to allegations of
4 copying and infringement in support of its secondary condition of
5 non-obvious arguments. As we see here on the bottom right,
6 GoSecure never got any discovery into any CrowdStrike platform.
7 They don't know how any data is stored in any CrowdStrike
8 platform. They simply have this visual depiction of, it's a little
9 hard to see on the slide, but orange nodes connected by purple
10 lines. Those, according to GoSecure, are the attack activity
11 sources, targets, and the purple lines are their associations. So this
12 depiction in CrowdStrike's platform, as I asked Dr. Stavrou,
13 GoSecure's expert, on cross-examination, Exhibit 1034, starting at
14 line -- I'm sorry page 43, line 24, how did you interpret the phrase
15 data structure in the -- in limitation 1C, purposes of assessing
16 infringement? I asked the question, is the graph database a data
17 structure? And the answer was yes. This is the graph database.
18 This is the level of detail they have. It is just nodes and
19 connections between those nodes.

20 Turning to DX 16, I took Dr. Stavrou to the intrinsic
21 record, the '872 Patent, and I said, does the patent provide an
22 exemplar of forensic data produced by the introspection module?
23 Yes, it does. He pointed me to figure 3A, the exact same
24 arrangement, a depiction of nodes and the connections between the
25 nodes. This is the information that is being collected by the

1 introspection module. This depiction of nodes and their
2 relationships is the data contained in the forensic data according to
3 Patent Owner's own expert, Dr. Stavrou. This is important, as I've
4 alluded to, because Capalik describes exactly that same process of
5 using an introspection module to monitor an attack, generate
6 forensic data, and then use that forensic data to generate a
7 signature of the attack that can be sent off to another computer
8 system.

9 JUDGE BAER: Capalik doesn't have a picture like that
10 on your DX 16, though, right?

11 MR. HART: Capalik does not -- coming back to DX 16,
12 figure 3A in the '872 Patent, Capalik does not depict the nodes and
13 the connections between the nodes in the way the '872 Patent, as
14 we talked about earlier. It also doesn't provide these exemplary
15 arrangements of data that we see in figures 5A and 5B in the '872
16 Patent. But if we go to DX 17, it is describing the exact same
17 system. I mean, the language between Capalik and the '872 Patent
18 with respect to how attacks are monitored, what data is generated,
19 and how that data is used, is nearly verbatim between the prior art
20 and the challenge patent. And, I'm sorry, DX 18 takes us to
21 Claims 1 to Claims 3, and this is an important point. As we just
22 saw in DX 17, introspection module creates the forensic data, and
23 then that forensic data, according to the patent, is used to generate
24 a fingerprint. That's exactly the structure of the claims. We have
25 in 1C, storing in the memory the data structure, and then in Claim

1 3, creating from that stored information a signature or a fingerprint
2 that is indicative of the attack.

3 So we have a parallel between the '872 Patent, its claims,
4 and Capalik's disclosures. They are all describing forensic data
5 generated from monitoring that attack and then taking that forensic
6 data and turning it into a signature. There is no meaningful
7 difference between what Capalik is describing and what is
8 described and claimed in the '872 Patent. Now, the suggestion,
9 and we covered this a little bit earlier, the suggestion from the
10 Patent Owner is that forensic data standing alone is insufficient.
11 There must be some additional process that needs to occur to
12 convert forensic data into the claimed data structure. So I explored
13 this position with Dr. Stavrou, Patent Owner's expert. I said, help
14 me understand, “your opinion is that the data structure required
15 Claim 1 uses the forensic data created by the introspection module,
16 but then organizes it in a different way. Is that right?” And he
17 said “it might require additional steps like processing, inference
18 I wouldn't know, because [this is not something that's
19 described by the patent.]” And I explored this, as you can imagine
20 -- explored this for quite a while with him, trying to understand
21 what we were dealing with here. I said, okay, the claim -- claimed
22 “data structure differs from the forensic data in how the data is
23 organized and presented. Is that right?” “[t]here is no clear
24 description here how you pass from the forensic data to the
25 [claimed data structure] . . . it's not clearly delineated [by the

1 patent] as far as I can tell.” That was Patent Owner's expert
2 position. There is something else required, but the patent doesn't
3 tell us what that is. The reason is that there is nothing else
4 required. The forensic data is the claimed data structure. It
5 includes all of the data that is recited in the claims. It is used in
6 exactly the same way that the claims require to generate a
7 fingerprint, and the description of an introspection module that
8 generates that forensic data and uses it to make a fingerprint is
9 nearly verbatim between Capalik and the '872 Patent. There's just
10 no meaningful delta between prior art and the challenge patent on
11 this issue.

12 Motivation to combine Capalik and Goal: I alluded to
13 earlier that it does not appear the Patent Owner is disputing that
14 Capalik's forensic data includes the activity sources, targets, and
15 their associations. Goel is part of this record solely to rebut a
16 position that Capalik is lacking in that respect. So I'm going to
17 hold this for rebuttal time and -- and see if I'm right about Patent
18 Owner's concession on that point. So that takes me to secondary
19 conditions. I alluded to this earlier, so Slide 23 addresses
20 secondary indicia of non-obviousness. There was a motion for
21 additional discovery in this case to try and get information about
22 how CrowdStrike's prior art platform worked. That was denied.
23 There is no information in this record about any particular
24 CrowdStrike platform. There's certainly no examples of how data
25 was stored, no examples of how it worked in any detail. So

1 without discovery into the -- any -- into any CrowdStrike platform,
2 no testimony from the designers, no evidence of revenues
3 generated by any particular CrowdStrike platform, and certainly no
4 feedback from any CrowdStrike customers discussing why they
5 went with CrowdStrike, what made them purchase any particular
6 CrowdStrike platform.

7 The Examiner argues that CrowdStrike copied the '872
8 Patent, and that the aspects copied from the patent, in isolation
9 from anything that is in Capalik, both drove the financial success
10 of CrowdStrike as a company and garnered industry praise. The
11 reality is the record does not substantiate any of this. There is a
12 woefully deficient record on which to find any of these three
13 elements: copying, commercial success, or industry praise with a
14 nexus to the '872 Patent in question. Monitoring all activity, claim
15 2 is a dependent of claim 1, and this is slide DX 25. Claim 2
16 additionally requires that the monitoring comprises monitoring all
17 activity on the first computer system. So this is the decoy system
18 where the attack has been -- has entered the system and is being
19 monitored. Capalik monitors all attack activity in its virtual
20 machine running on the decoy device. That is what claim 2 is
21 talking about. That is what the intrinsic record is describing with
22 respect to these embodiments that monitor all activity in lieu of
23 monitoring for only certain things. There are certainly
24 embodiments in the '872 Patent that talk about holding off on the
25 monitoring until some key system call is detected rather than

1 monitoring all attack activity, that in 100 percent of the
2 embodiments, the monitoring in the '872 Patent is limited to
3 monitoring attacks and monitoring attacks that are running on a
4 virtual machine and monitoring those attacks on a virtual machine
5 that is running on a decoy device. And in that respect, Capalik is
6 identical. It teaches exactly that same process of assuming
7 everything is suspicious and monitoring everything.

8 JUDGE POWELL: So, the device that does the
9 monitoring -- I believe it might have been processor 508 -- I think
10 I understand your position to be that you prevail on claim 2 even if
11 508 doesn't -- isn't monitored because the claim, the proper
12 construction of this dependent claim, is that it doesn't require
13 monitoring outside of the virtual machine. Does -- is that?

14 MR. HART: That's exactly right. And it really comes
15 back to what is the activity that this claim requires to be
16 monitored. And it's very clear in the context of the claim and
17 certainly in the context of the '872 specification: it is attack
18 activity, right? You're not monitoring the modules that are doing
19 the monitoring. There's no turns all the way down where
20 monitoring is monitoring -- monitoring over and over again. It's
21 always attack data. These are decoy devices in every embodiment.
22 The attacks are running on virtual machines in every embodiment,
23 and the only thing being monitored is the attack activity as it
24 occurs on those virtual machines.

25 And so interpreting monitoring all activity in light of the

1 intrinsic record requires us to conclude that what is being
2 described here is monitoring all attack activity. And the patents do
3 distinguish between embodiments. There are embodiments where
4 all attack activity, as soon as an attack comes in, everything's
5 monitored. There are other embodiments where, as soon as an
6 attack comes in, you're waiting for a trip, you're waiting for a key
7 system call before you start monitoring because it may not be
8 worth monitoring if it's a benign some -- you know, a worm that is
9 just exploring the virtual machine but hasn't done anything that
10 could cause harm yet. And so those are the two distinctions, the
11 two different types of embodiments: either monitoring only some
12 attack activity or monitoring all attack activity. But in 100 percent
13 of the embodiments, you are only monitoring attack activity.
14 That's what the monitored activity is in these claims.

15 JUDGE BAER: And what is the disclosure in the prior
16 art of this monitoring? I believe it was -- it was relatively terse,
17 wasn't it?

18 MR. HART: It was relatively terse. It -- it essentially
19 said, and I may have that. Essentially says when the attack comes
20 in, so when an attack comes in the port and is detected, in some
21 embodiments the introspection module monitors that attack as it
22 occurs. Essentially, it says everything that happens -- the
23 keystrokes, the system calls, the call generation -- is monitored by
24 that introspection module. So it does not -- it does not as clearly
25 delineate between the possibility of waiting for a key system call,

1 but it certainly teaches that once that attack comes in, you are
2 monitoring.

3 JUDGE BAER: Yeah. I'm just a little confused because
4 I thought the dispute was over whether every activity was
5 monitored or whether the entirety of each activity was monitored,
6 but I'm not sure that is your position. Could you clarify that for
7 me?

8 MR. HART: Absolutely, Your Honor. The dispute is
9 whether there needs to be monitoring. So the first computer
10 system that we've mapped in claim 1 is the decoy device. The
11 structure of the claim requires memory. It requires processors. It
12 requires hardware that does not exist in a virtual machine. So the
13 entire first decoy device is the first computer system. This claim
14 requires "monitoring all activity on the first computer system."
15 Patent Owner has taken the position that if we have mapped the
16 decoy device as the first computer system, that we have to show
17 Capalik monitors everything that happens on that decoy device
18 even outside the virtual machine and even unrelated to attack
19 information. That is not what these claims are talking about.
20 These claims are focused on monitoring attacks. It's attacks on
21 virtual machines. There is no delta between what Capalik is
22 describing with respect to monitoring attack activity on a virtual
23 machine and what is described in the '872 Patent. The '872 Patent
24 does not monitor outside the virtual machine. It does not monitor
25 anything other than attacks.

1 JUDGE POWELL: Okay. So within the virtual machine
2 in Capalik, it is possible that there are non-attack related activities
3 that are not monitored. How does -- what's Petitioner's position on
4 that?

5 MR. HART: Within the virtual machine -- the virtual
6 machine --

7 JUDGE POWELL: On Capalik, yeah. Inside the virtual
8 machine.

9 MR. HART: In -- in both the '872 and in Capalik, the
10 virtual machine exists to be attacked.

11 JUDGE POWELL: Right.

12 MR. HART: It -- it waits until something comes to it and
13 then it pretends that it is a normal operating system that is using
14 normal hardware and tries to convince the attacker that it is a
15 normal computer system. So there is nothing going on until there
16 is attack. That's the whole point of these inventions of using a
17 decoy system with a virtual machine that to attackers appears to be
18 a normal computer is so that you can incentivize attacks, appear
19 normal and not scare them away so you can monitor what they're
20 trying to do.

21 JUDGE POWELL: Okay. Thank you. But the
22 whenever disclosure from Capalik is a disclosure of which attacks
23 are monitored, not the substance of the attack, as I understand it.
24 Do I have that right?

25 MR. HART: It -- there is no suggestion by Capalik that

1 you would monitor something less than everything. So the -- when
2 Capalik describes starting to monitor at the detection, essentially a
3 trigger of the attack arriving, it says that everything is being
4 monitored. It doesn't distinguish between monitoring for certain
5 things and monitoring everything. Its introspection module
6 captures all keystrokes, all file modifications, everything that
7 happens as part of that attack.

8 JUDGE POWELL: Where is that disclosure in Capalik?
9 Because when I looked at your petition and your mapping for
10 claim 2, I don't -- I see the whenever citation, but I'm not seeing
11 the information as far as the content of what is monitored. And I
12 understood you to just say, well, it doesn't say anything is not
13 monitored, but I'm looking for something affirmative that it does
14 say regarding the content of that monitor.

15 MR. HART: Yes. So our expert elaborated on this in
16 paragraph 145 and 146 of Exhibit 1003. He cited Capalik at
17 paragraph 59, which is the whenever language you just read into
18 the record. “[W]henEVER data is found to be transferred through a
19 socket,” the processing module “may generate a signature.”

20 He also quoted paragraph 49 that describes the operation
21 of the introspection module. “When an attacker connects through
22 a network port and begins interacting with a [virtual device],
23 introspection module 538 monitors and captures information from
24 the connection, including port numbers, data streams, file
25 uploads,” et cetera -- et cetera. The POSITA would've understood

1 Capalik's detailed forensic data monitors all activity on the
2 computer system that begins with a connection through a virtual
3 machine network port. And he goes on to explain the
4 understanding in the art of how these honeypots, these systems that
5 are designed to incentivize attacks, are designed to operate. They
6 are incentivizing that attack so that attack can run and be
7 monitored by the systems.

8 So this is the detailed explanation of how Capalik's
9 disclosure interpreted by a POSITA satisfies monitoring all attack
10 activity once that attack is detected.

11 JUDGE POWELL: So it's your position that it monitors
12 every attack and that it monitors all substance of every attack. Do
13 I have that right?

14 MR. HART: You have that right, Your Honor.

15 JUDGE POWELL: And the -- all substance comes from
16 paragraph 49. Do I have that right?

17 MR. HART: Yes, that is the operation of the
18 introspection module that does the monitoring, that generates the
19 forensic data.

20 JUDGE POWELL: The other citations are to the every
21 attack piece. Do I have that right? In other words, the whenever
22 clauses indicate that every attack is monitored, not the substance of
23 the attack. Do I have that right?

24 MR. HART: You do have that right, Your Honor.

25 JUDGE POWELL: And did you take a position or are

1 you prepared to take a position now that it doesn't matter even the
2 content of the activity, so long as every -- excuse me, every
3 activity is monitored, that is sufficient given a proper claim
4 construction of claim 2?

5 MR. HART: I want to make sure I understand your
6 question. You're asking if we are willing to take position that
7 claim 2 is satisfied if --

8 JUDGE POWELL: There are no activities that get
9 through that aren't somehow monitored.

10 MR. HART: The -- the claim 2, yes, in the virtual
11 machine, everything that occurs after the attack enters that port is
12 being monitored, and that is what -- what is required of claim 2.
13 There may be -- there may be virtual machine monitor activities,
14 fingerprint generation, transmissions that occur on the decoy
15 device outside of the attack as it's running on that virtual machine.
16 But that virtual machine is designed to be a self-contained apparent
17 operating system by the attack, and the introspection module
18 monitors everything that happens as part of that attack, and that is
19 what claim 2 requires.

20 JUDGE POWELL: Thank you.

21 JUDGE WHITE: Okay. Counsel, I know you're getting
22 to your rebuttal time, but just on the flip side of that, what -- when
23 does Capalik do when it runs into benign activity, just so that I
24 understand sort of the context of what's happening and when is it
25 doing its monitoring? So when a benign transmission comes

1 through, what's -- what's -- what happens?

2 MR. HART: So Capalik does contemplate the possibility
3 of not needing to generate a signature or a fingerprint if when it
4 analyzes that forensic data and determines that nothing went
5 wrong, that it doesn't need to generate anything and send that on to
6 a protected network. But it does not -- it does not distinguish
7 between monitoring everything with the introspection module and
8 waiting for something dangerous to occur in the same way the
9 '872. So claim 2 is the embodiment being described by Capalik,
10 where everything is monitored. If there was a corollary or a -- I'm
11 missing the word I'm looking for here -- but if there was a claim
12 2.5 that said monitoring only certain activities as defined by the
13 system, that is not something that -- that Capalik expressly
14 contemplates in the way the '872 does.

15 JUDGE POWELL: You're -- you know, I think --

16 MR. HART: I know I'm over, yes.

17 JUDGE POWELL: Yeah, and that's fine. Just so you
18 know how much time you've got left, which is about a minute.

19 MR. HART: It's unavoidable, Your Honor, but I do
20 appreciate the warning. I will very -- what we have remaining are
21 a few dependent claim issues. So I'll quickly go through these.
22 Claim 8 is a dependent on claim 7. Claim 7 depends on 1. Claim
23 7 says graphically displaying at least a subset of stored activities,
24 and claim 8, visually distinguishing at least a subset of the
25 associations within activities. So what we have relied on really is

1 on the right in DX 29. That is figure 3.2C from King. This is
2 what's referred to as a filtered dependency graph that is generated
3 by King. It is our position that when King -- or when King
4 displays that filtered dependency graph, that graph represents only
5 associations that have been assigned the type malignant. So it has
6 removed any benign associations, and we see that if I come back to
7 DX 29, we've provided annotations. The full attack is figure 3.2B.
8 In here, we've annotated benign associations in green. The process
9 in King takes those benign associations away, providing a -- a
10 filtered dependency graph that is just malignant. Essentially, the
11 idea is you only want to know what mattered for purposes of
12 assessing the attack. What is related to the harm that that attack
13 caused? So when you have removed those benign associations and
14 displayed only what remains, which is malignant, that satisfies
15 both claim 7 and claim 8. As we saw in 4.3C, that figure
16 graphically displays at least a subset of the stored activities, and it
17 also visually distinguishes at least a subset of the associations. It is
18 displaying only those associations that have been deemed type
19 malignant, satisfying 7 and 8. Turning to determining an activity
20 status, this is on DX 31. This dependent claim requires
21 determining a complete status where every target of an activity is
22 associated with a source. This too, we point to the process of
23 generating that filtered dependency graph in King 3.2C. As we
24 explained in our papers, that filtered dependency graph is
25 generated only after King has determined that it has a source for

1 every target, so it can assess each of those associations in order to
2 filter out the benign associations and arrive at a filtered graph
3 showing only malignant associations, essentially what was
4 important to the attack. Claim 19, the association includes an
5 attack. Again, we are relying on King's filtered dependency graph
6 process. King features taking that stored information about the
7 attack, which in our combination is Capalik's forensic data, and
8 using that to filter out any benign associations. So it is
9 determining a malignant type from the forensic data stored by
10 Capalik, satisfying dependent claim 19. Finally, Pike's DEP. The
11 claim recites claim 13, dependent claim 13 that starts on DX 36,
12 identifying activity sources that request to access a portion of
13 memory that is set as non-executable. In the '872 Patent, it
14 describes a non-executable memory as part of a DEP process. Pike
15 is teaching that same non-executable memory process. In both
16 Pike and the '872 Patent, there is an exception or a trigger that is
17 created when the system detects that something is trying to access
18 that non-executable memory. The purpose of that trigger or that
19 exception is to ensure that no harm comes from that. So in both
20 cases, Pike's DEP process and the '872 Patent's DEP process, you
21 are looking for an attempted access of non-executable memory, so
22 you can trigger an exception and shut that down to prevent harm.
23 Unless there are any questions, I will try to reserve the rest of my
24 time.

25 JUDGE POWELL: I think we're good.

1 MR. HART: Thank you.

2 JUDGE POWELL: So, you have just short of seven
3 minutes left. How much time would you like?

4 MR. PATHMANABAN: We'd like to reserve 15
5 minutes, Your Honor.

6 JUDGE POWELL: Okay.

7 MR. PATHMANABAN: Thank you.

8 JUDGE POWELL: Adjust the clock here, and we look
9 forward to hearing your arguments when you're ready.

10 MR. PATHMANABAN: Thank you, Your Honors. I
11 will -- my name is Giri Pathmanaban again. I will be addressing
12 Ground one, that is specifically claims 1 and 2, and my colleague,
13 Mr. Peters, will address the remaining Grounds, subject to time
14 availability, of course. There was a lot of time Mr. Hart spent on
15 the similarities between Capalik and the '872 Patent. And of
16 course, they do share a common inventor, and they both originated
17 from GoSecure's predecessor. So this is the -- Capalik patent
18 application is GoSecure's patent -- patent application as well.
19 However, I want to focus you on the differences. I'm on slide 4. I
20 apologize, Your Honors.

21 JUDGE POWELL: That's okay.

22 MR. PATHMANABAN: I'm going to try to remember
23 to call out our slide numbers. I'm on slide 4 --

24 JUDGE POWELL: Actually, I'm sorry. I think we've
25 got a technical difficulty, I believe. I'm -- yeah. Sorry. Stop the

1 clock here, and -- and I think the communication line to Dallas
2 seems to be frozen.

3 MR. PATHMANABAN: Okay.

4 JUDGE POWELL: We're working on it. I very much
5 apologize.

6 MR. PATHMANABAN: No problem, Your Honor.

7 JUDGE POWELL: Yeah, let's go off the record.

8 THE CLERK: We will.

9 JUDGE POWELL: Okay, let's go back on the record.
10 And we'll -- I'll start the clock again when you're ready.

11 MR. PATHMANABAN: I'm ready, Your Honor. Thank
12 you. So I want to focus on the differences between Capalik and
13 the '872 Patent, which Mr. Hart glossed over. And I recall he said,
14 I think at least twice, that there are imaginary disclosures in the
15 '872 Patent. Well, here's the disclosure, figures 3A to 3C, which
16 he showed you, he questioned our expert about. These figures, 3A
17 to 3C, they are in the '872 Patent. You know where they're not?
18 They're not in Capalik. No. Nowhere. This is not an imaginary
19 disclosure. This is a data structure. It's a tree data structure. It
20 -- the data structure is a structured representation of data. It can, of
21 course, take many forms, like a tree; it can take a structured list; it
22 can take a table, but none of these structures are in Capalik
23 whatsoever. In this figure 3A, we have packet stream, an attacker
24 who's sending in a packet stream. That's the source. And by the
25 way, those labels are from the patent. I didn't add anything. I just

1 added the coloring. I'm on slide 6. And the packet stream is
2 coming in source. There's an association between what's the action
3 being taken and then there's the target. That's the socket. Figure
4 3A. Then it goes on to 3B and 3C, and it's talking about where all
5 this data is promulgated and the attack is promulgated. None of
6 this stuff is in Capalik whatsoever. Yes, there is some similarity in
7 terms of forensic data, but that's not all in the '872. The '872
8 Patent, starting from the very title to multiple figures, multiple
9 columns of text, and of course, most importantly, the claims, is
10 talking about a data structure that identifies a source, a target, and
11 an association between the two. None of that is in Capalik. Mr.
12 Hart spent a whole lot of time talking about the introspection
13 module and forensic data, but forensic data is not a data structure.
14 Nowhere in the '872 Patent is it equating the two. In fact, it's
15 distinguishing the two. Yes, you can generate a signature from
16 pure forensic data. That's true. Capalik does that. The '872 has
17 the same disclosure. But that's not what's claimed. What's
18 claimed and what's on these embodiments, which are not in
19 Capalik at all, like for example, Figure 5A -- this is a table, again,
20 talking about data structures. And nowhere, when it's referring to
21 data structures, is it ever -- and Mr. Hart didn't show you anywhere
22 -- where the '872 Patent is equating the data structure to raw
23 forensic data. You can have raw forensic data, Your Honors, and
24 that is not a data structure. And specifically, I want to be -- be
25 careful here. It's not just a --

1 JUDGE BAER: And would --

2 MR. PATHMANABAN: Sorry, Your Honors. Go -- go
3 ahead.

4 JUDGE WHITE: Would you --

5 MR. PATHMANABAN: Do you have a question?

6 JUDGE WHITE: Yes. What -- what Petitioner seems to
7 be pointing to is a relational database.

8 MR. PATHMANABAN: I was getting right to that
9 point, Your Honor.

10 JUDGE WHITE: Okay. So my question is, is a
11 relational database not a data structure within the claim -- within
12 the claim limitations?

13 MR. PATHMANABAN: So, a relational database could
14 be a data structure, but the claim requires a data structure that
15 identifies the activity sources, the activity targets, and the
16 associations for the plurality of activities. Nowhere is there any
17 disclosure in Capalik of this relational database storing for each of
18 identified activities, okay? For each of a plurality of activities, it
19 has to have this data structure identifying the sources, the targets,
20 and the associations for the plurality of activities. Nowhere is that
21 disclosed. All it's talking about is we store raw attack information
22 in this relational database. There are many different ways you
23 could store that. You could store that without any structure
24 whatsoever in the relational database. You could have one basic
25 field that stores all of it. And of course, you can generate a

1 signature from it. That does not mean that it is disclosing a data
2 structure that identifies the activity sources, the activity targets,
3 and the associations for the plurality of activities.

4 JUDGE WHITE: Why wouldn't one field that stores all
5 that satisfy that if that's what the structure was?

6 MR. PATHMANABAN: Because it needs to identify
7 -- it needs to have some organized way of identifying this
8 information, like we see in these figures, multiple figures from the
9 '872 Patent. Let me just go there. I'm going to -- I'm sorry. Slide
10 22. On the left, I have the '872 Patent, and you've got figures 3A
11 through 3D, figures 4A through 4E, all of which are showing what
12 are well-known data structures, tree structure, graph nodes, and
13 tables. None of this is in the Capalik reference, and this is not
14 -- we're at --

15 JUDGE WHITE: Okay, Counsel, here's what I need you
16 to walk me through.

17 MR. PATHMANABAN: Yeah.

18 JUDGE WHITE: What I see in the language is a data
19 structure that identifies the one, two, three things listed. So if you
20 have a data structure that just includes those three things, whether
21 it be one field or three fields, why would that data structure not be,
22 sufficient, if it doesn't specify how that data structure is supposed
23 to be structured? So if there's one field that includes those three
24 bits of information within it, why wouldn't that satisfy?

25 MR. PATHMANABAN: Because it's just raw data. If

1 you look at Capalik's -- you could have raw data from which you
2 can presumably derive some information out of it, but it is not
3 structured in this way.

4 JUDGE WHITE: Okay. Now I think we're getting down
5 to something. So -- so you're saying that it -- it can't be raw data?

6 MR. PATHMANABAN: Correct.

7 JUDGE WHITE: How is it raw data if it's stored in a
8 field in a database? Wouldn't that render it no longer just raw data
9 because it is in a structure? You're -- you're not just getting a
10 string of information. You have a field that says whatever it needs
11 to say with -- to include these three things. Why would that not be
12 a data structure and why would that be raw data?

13 MR. PATHMANABAN: Well, then, Your Honor, if -- if
14 it could just be one field that has this data dump, that would be no
15 difference between a data that identifies these three things versus a
16 data structure that identifies these three things. And there is a
17 difference there. That's what the '872 Patent is all about. The --

18 JUDGE WHITE: Well, let's take a look at the database.
19 I associate that, and I think one of ordinary skill in the art would
20 associate that with the structure of a relational database, columns
21 and fields. I mean, column and rows. So there's -- if it's in a
22 relational database, it has to have some structure of columns and
23 rows, does it not?

24 MR. PATHMANABAN: Well, first of all, I want to be
25 --

1 JUDGE WHITE: Okay.

2 MR. PATHMANABAN: There is no disclosure in
3 Capalik whatsoever that this database includes all of these things,
4 these three things. None. It just says it stores for forensic attack
5 information, okay? There is no disclosure that it includes these
6 sources, targets, and associations.

7 JUDGE WHITE: So then, is -- am I understanding your
8 position then to be that there may be a relational database, but that
9 relational database is insufficient because it does not store the
10 correct information?

11 MR. PATHMANABAN: There's certainly absolutely no
12 disclosure in Capalik from which a person skilled in the art can
13 -- can say it discloses a database that has these three things.

14 JUDGE WHITE: Okay, thank you.

15 MR. PATHMANABAN: I'm looking at slide 17, Your
16 Honors. Their position, and Mr. Hart reiterated it multiple times in
17 his argument, is because Figure 3C depicts nodes and associations
18 -- and he's talking about, this is from Petitioner's reply, Figure 3C.
19 They're referring to Figure 3C of the '872 Patent, not Capalik.
20 Because Capalik teaches the same functionality using nearly
21 identical -- identical language, its forensic data similarly identifies
22 the claimed data structure. So let's be clear about what they're
23 arguing here. This is the epitome of hindsight. They're saying
24 simply because there's overlap in some disclosures between
25 Capalik and the '872 Patent, Your Honors can use the disclosure of

1 the '872 Patent, meaning Figure 3A, 3B, 3C, to gap-fill Capalik
2 and essentially invalidate the '872 Patent. This is classic hindsight
3 of the highest order. Figure 3A doesn't appear in Capalik. 3B
4 doesn't appear in Capalik. 3C doesn't appear in Capalik. None.
5 Zero. It just has raw attack information.

6 JUDGE BAER: But when you say raw attack
7 information, Counsel, do you -- could you explain what you mean
8 by raw data? Because if -- if you could square that with Capalik's
9 disclosure at paragraph 49 when it describes the content of that
10 data, that would be helpful.

11 MR. PATHMANABAN: Yes, Your Honor. The -- it's
12 talking about this forensic data that it collects from when there is
13 an attack. When the virtual machine is attacked, it collects data
14 about that attack. That all is just stored. There is no disclosure
15 whatsoever of storing it in a data structure with the three required
16 things: source, targets, and associations.

17 JUDGE BAER: Okay.

18 MR. PATHMANABAN: Such as in the -- in the '872
19 Patent, excuse me.

20 JUDGE WHITE: So is it your position that -- that when
21 we're reading Capalik, we -- we think that because everything
22 that's listed in that -- we think that everything that's listed in 49 is
23 what's being stored in the relational database? Is that not within
24 the relational database?

25 MR. PATHMANABAN: I'm just going to, if you don't

1 mind. I'm just going to look at Capalik paragraph 49. And
2 paragraph 49 says, Monitors and captures information from the
3 connection, port numbers, data streams, file uploads, keystrokes,
4 ASCII or binary files, malicious payloads, memory manipulation
5 attempts, and any other data transfers or malicious attempts.
6 That's all. It collects that data, yes. Does it, from that data, then
7 derive this structured data of here -- here's the source for that, for
8 that attack, here's the target, here's the association, and does that
9 for every -- excuse me, every identified activity? No. That
10 disclosure is not there. That's what's required by 1C. And slide
11 18, Petitioner's position is the claims do not impose any specific
12 structure of the stored data. And -- but again, please focus on the
13 actual language. The language is a data structure that identifies the
14 activity sources, the activity targets, and the associations for the
15 plurality of activities. And the plurality of activities is referring
16 back to the identified activities in step 1B. So for each of those
17 activities, you've got to have a data structure that identifies these
18 three things. Where is that in Capalik? It's just not there.

19 JUDGE BAER: Go ahead. I think I heard that you're not
20 saying there has to be a separate data structure for each activity.

21 MR. PATHMANABAN: No.

22 JUDGE BAER: Okay.

23 MR. PATHMANABAN: That -- that's no.

24 JUDGE BAER: Okay. okay.

25 MR. PATHMANABAN: No, that's not my point, Your

1 Honor.

2 JUDGE BAER: Is it your position that the data in
3 Capalik is unstructured, or that the data in Capalik may be
4 structured but that structure does not identify the source, target,
5 and association?

6 MR. PATHMANABAN: It is unstructured, Your Honor.
7 It is just forensic data. That's all it says. From that forensic data, it
8 derives a fingerprint. And by the way, the -- the fingerprint is not
9 -- they don't claim as a data structure. They can't because they
10 argued elsewhere -- this is on slide 20. This is from the petition.
11 They said that the fingerprint of the '872 Patent can include one or
12 more of an activity source, target, and other descriptive data of an
13 identified attack. And Capalik expressly teaches generating a
14 fingerprint of an attack that identifies the port targeted by the
15 attack. In other words, that fingerprint in Capalik is disclosing the
16 target. That's what they argue. They never argue that the
17 fingerprint identifies each of those three things, and it certainly
18 does not.

19 JUDGE BAER: I'm just trying to understand whether
20 you're saying this is a box drawing problem and that they've drawn
21 the box in the wrong place, or are you saying that it doesn't matter
22 where you draw the box -- the -- this structure doesn't exist at all.

23 MR. PATHMANABAN: It -- it does not exist, Your
24 Honor. The -- this is not a box drawing exercise. This is the
25 fundamental difference. The data structures are the -- that, and, of

1 course, element 1D that I will get to is the fundamental difference
2 between the Capalik patent and the '872 Patent. It's why we didn't
3 file this—our client didn't file the '872 as a continuation of the
4 Capalik reference, which, of course, they could have. But this, the
5 '872, is an entirely new invention about data structures that are
6 used to generate data structures to represent data and store data,
7 and then from that you derive information that is sent to other
8 computer systems to protect those computer systems.

9 JUDGE WHITE: So just so I am clear are you saying
10 that the source target and associations are in that raw data in
11 Capalik, or they're not in that raw data?

12 MR. PATHMANABAN: Well, it's -- it's not at all clear
13 what's in or not in that raw data, Your Honors. The point is they
14 have -- they have to show that it's in there, and they have to show
15 it's in there for every identified activity and that it's in a data
16 structure. They've simply not done that because it's not there. And
17 there was a lot of discussion by Mr. Hart about what he asked our
18 expert and what he said about the forensic data. To be clear, yes,
19 the '872 Patent only twice talks about forensic data as well, but it
20 never ever attaches that term to figures 3A through 3C, 4A through
21 4E, 5A through 5C -- none of that. And that's what Mr -- Dr.
22 Stavrou was very clear about. He asked, “[d]oes the '872 Patent
23 describe Figure 3 as raw forensic data?” Answer: “No.” “Did
24 you intend to equate raw forensic data in the '872 Patent with a
25 graph form or structure that's shown in figure 3A?” “No.” That's

1 his clear testimony. And regardless, you can examine Figures 3A
2 and the accompanying text and all the other figures and the
3 accompanying text in the '872 Patent. Your Honors are very
4 diligent. I'm sure you will do that anyway, and you can examine
5 that as much as you want, Your Honors. You will not find a single
6 instance where those figures are equated to raw forensic data. No,
7 that's a fundamental difference between Capalik and the '872
8 Patent. I will go to limitation 1D if there are no other questions
9 about 1C.

10 JUDGE WHITE: One more on my part.

11 MR. PATHMANABAN: Yes.

12 JUDGE WHITE: So, I don't know if you have access to
13 Petitioner's demonstrative, but one of Petitioner's demonstratives
14 was the one where they compared the language of the '872 and
15 Capalik.

16 MR. PATHMANABAN: Yeah.

17 JUDGE WHITE: And in the comparison, it's not just
18 that the language is similar. It is -- it is nearly point for point as far
19 as what they're saying is being captured and what is being stored.
20 What is missing in -- in that -- in that description there that you're
21 saying is the -- is the thing that -- that shows that what you guys
22 are saying in your view that is totally different?

23 MR. PATHMANABAN: Yes, thank -- thank you, Your
24 Honors. I have the slide up. This is DX 17 from Petitioner.

25 JUDGE WHITE: Yes.

1 MR. PATHMANABAN: What is missing is very
2 important. What is missing is the data structure. You can see that
3 yes, they're pointing to the similarities, the introspection module
4 and the collection of forensic data and the fingerprint generated
5 from that forensic data. There is no description, not once, in these
6 columns of data structure because it's not there. That's a different
7 disclosure in the '872 Patent. Yes, it's there, but the '872 then goes
8 on to talk about all these data structures, which is not in these
9 columns. And you cannot just say -- again, this is the epitome of
10 hindsight -- oh, these columns are similar, so you can infer all this
11 other text, all these other figures, and the claims are by necessarily
12 disclosed in Capalik.

13 JUDGE WHITE: Would you agree that the term data
14 structure is one that is known in the art? It's a well-known term in
15 the art.

16 MR. PATHMANABAN: Yes.

17 JUDGE WHITE: Okay. So both parties agree that data
18 structure is in itself a well-known term of art. Do -- is it your
19 position that -- that any specific data structure is required by the
20 claim language?

21 MR. PATHMANABAN: No. There can be different
22 types of data structures, tables, arrays, graphs, trees, nodes. But
23 we can also agree what is well-known in the art is raw or -- or just
24 forensic data. No one would call forensic data a data structure. I
25 don't think so. And there is no evidence in the record that forensic

1 data is data structure.

2 JUDGE WHITE: All right, I think I have your position.

3 MR. PATHMANABAN: Thank you, Your Honor. So
4 I'm going back to Patent Owner's slides, our slides 23. Now I'm
5 going to focus on limitation 1D. And this limitation requires
6 transmitting to one or more computer systems other than the first
7 computer system, information identifying the activity sources,
8 targets, and associations for preventing future attacks to the one or
9 more computer systems. So what's really important about this
10 claim language is that the target of the transmission is: you are
11 sending this information for preventing future attacks to the one or
12 more computer systems. So you're transmitting to the one or more
13 computer systems to prevent future attacks on those computer
14 systems. What is undisputed about Capalik -- I'm going to jump
15 around a little bit. Excuse me. This is -- I'm on slide 31. Let me
16 just make this full screen. I'm on slide 31.

17 What's clear about Capalik's disclosure, I don't believe
18 there's a dispute about this, is that the data, the -- the fingerprint or
19 signature, is sent only to an IDS, intrusion detection system. It
20 does not reach those protected network devices on top, the 536.
21 And what is also clear, and there's no dispute about this either, is
22 that the protected network devices are the ones that you're
23 preventing future attacks for. The patent is clear. There are two
24 different embodiments disclosed, and I believe Judge Powell asked
25 this question. There are -- I'm on slide 25. There are two different

1 embodiments disclosed. One is sending, transmitting signatures to
2 an IDS, IPS system to prevent future attacks to the one or more
3 protected network devices. And the other is transmitting that
4 information, the -- the signatures, to the protected network devices
5 themselves. Judge Powell asked a -- a very interesting question,
6 which was that does the patent ever disclose equating this
7 introduction -- excuse me, IDS with a computer system? And the
8 answer is no, it does not. Now Mr. Hart replied, Well, it doesn't
9 equate an endpoint, a protected device, with a computer system as
10 well. What it does say in both embodiments is you send this
11 information to protect the protected devices, to prevent future
12 attacks on the protected device. Both of those embodiments, the
13 devices that are protected from future attacks are the endpoint
14 devices. Okay? It would have been easy for the inventors to claim
15 a system that said, transmitting information to protect computer
16 systems, period. But they specifically said, transmitting to one or
17 more computer systems other than the first computer system,
18 information for preventing future attacks to the one or more
19 computer systems. You're transmitting to the systems that are the
20 subject of the attack, not to an IDS, IPS system. We asked -- I'm
21 going to go to slide 30.

22 We asked their expert. The problem with the
23 construction that they propose, and respectfully, we understand the
24 board agreed at the institution stage, the problem is it would be
25 simply an arbitrary box drawing exercise. He says, so think

1 -- think of a computer system as dough. You're baking a bread,
2 right? So computer system could be all of the dough. It's, you
3 know, every computer on Earth and the internet and all the routers
4 on the internet. You could also cut off a piece of your dough, you
5 know, form a bun. That's a computer system that comprises all the
6 devices in your home. Computer system is a little bit like dough.
7 You could cut it in different places and say, Identify this portion.
8 This, of course, is dough. This is a computer system. So in other
9 words, what he's saying is, you could cut it whatever way you
10 want. That leaves the claim impermissibly ambiguous. Nobody
11 knows what is and what is not one or more computer systems that
12 is not the first computer system. It's just I'll call it when I see
13 -- when I see it. That cannot be a proper construction, we would
14 submit, Your Honors.

15 JUDGE BAER: What do you think about Petitioner's
16 stance that the express descriptions of the various components in
17 the claim connecting to certain other components and sending
18 things to certain other components sort of obviates the concerns
19 that -- that it's all just unbounded?

20 MR. PATHMANABAN: Well, I would say, I mean, just
21 look at -- at their drawing, their box drawing exercise for purposes
22 of this claim. I'm going back to slide 31 and the Capalik figure.
23 We don't think the Petition ever, by the way, ever said sending to
24 an IDS is enough. They did not say. They did not say in their
25 petition that IDS is part of the computer system to be protected. In

1 response to our POPR, they came back and said, oh, well, you
2 know what, computer system can be so broad it includes IDS
3 anyway. So, by that logic, why not include box 508? What's
4 stopping box 508 from being part of the computer system to be
5 protected? It's just a box drawing exercise. It's arbitrary. They
6 don't get to draw a box simply because it suits their purpose.
7 That's not what the claim is about. If it was so broad, the claim
8 could simply have been -- have said, transmitting information for
9 preventing future attacks on the one or more systems, and it
10 doesn't specify where to transmit that information. You would get
11 the same result. To the extent if their construction were true, you
12 would get to the same result if the claim simply said, transmitting
13 information to prevent future attacks on the one or more computer
14 systems other than for services.

15 JUDGE WHITE: Counselor, the way I understand
16 Petitioner's position is not that they are arguing that that is the
17 outer limit of anything. That I understand their position to be that
18 the claim is at least as broad enough to include the IDS, IPS
19 system, not that it is boundless and can include all things. So with
20 the thought in mind that they are not arguing that that is that -- that
21 this is an outer limit, merely that it is broad enough to include the
22 IDS system, why is that not for the purposes of this proceeding,
23 why is it not a concrete enough definition for us -- for this?

24 MR. PATHMANABAN: Respectfully, Your Honors, I
25 mean, they have not articulated any rationale for how they divide

1 the claim then. If you look at their DX 11, they're saying this
2 distributed computer system, Figure 1 -- that's a computer system.
3 The entirety of -- of all computers, including the internet, is a
4 computer system according to them. So they could just box draw
5 around any box in Figure 1 and call it one or more computer
6 systems. That's their position.

7 JUDGE WHITE: Okay. Let's -- let's look at it this way.
8 What we're required to do is to construe the claim at least enough
9 to resolve the dispute before us. So we don't have to resolve
10 everything, but we need to resolve enough to know whether what
11 they are saying is sufficient. So whether the IDS system is
12 sufficient, we need to resolve enough of the claim. I don't know
13 that -- that the Petitioner has given us an outer limit to the claim. I
14 wouldn't say that they have. I think they're just saying that there is
15 an outer limit. It's not, of course, you know, taking every
16 computer, every -- I don't think either party would say that -- that
17 is a -- a proper viewing of the claim term that it includes
18 everything everywhere. But I think that they are taking a position
19 that's a little narrower than that, that it's broad enough to include if
20 -- why is that not a sufficient definition or construction for the
21 purposes of this proceeding?

22 MR. PATHMANABAN: What is -- then I don't
23 understand, Your Honor, what is the principle behind including the
24 IDS in Capalik's -- the Capalik's IDS as part of the protected
25 computer network, why is that protected computer network by

1 itself one or more computer systems, whereas the -- the rest is not?
2 How do you distinguish that? How do you draw that line? What's
3 the principle? I don't understand it. The -- the only principle
4 they've articulated, as far as I can tell, is computer system is a very
5 broad term that would encompass any number of computers.

6 JUDGE POWELL: Do you think that the proper
7 construction of computer system would encompass some range of
8 componentry? Is it limited just exactly to a computer, or does it
9 have some range that -- that it could refer to some computer
10 components?

11 MR. PATHMANABAN: I think it could -- yes. We're
12 not saying that strictly it's limited to -- you know, it -- it doesn't
13 exclude some components, for example. If you have a CPU
14 separate from a monitor, it doesn't mean that, you know, that's a
15 -- those are different devices. That's not our position. Yes, there
16 could be some range. And -- and I think the limiting principle is
17 really it has to be a computer system to be protected to prevent
18 future attacks on those computing systems that -- that is the subject
19 of the transmission that's receiving the transmission of
20 information.

21 JUDGE POWELL: Does every component of the
22 computer system that's to be protected have to be vulnerable? So
23 let's -- let's use your example there: a -- a CPU and a monitor. If I
24 say computer system would read on a CPU and a monitor -- and
25 the monitor -- I'm not as well-versed in all this stuff as your expert

1 is, I'm sure -- but the monitor maybe arguably is not vulnerable,
2 but the -- but the CPU is. Does the fact that the monitor itself is
3 not vulnerable mean it's not a computer system to be protected
4 within the meaning of the claim?

5 MR. PATHMANABAN: Well, I guess that depends on
6 what you mean by the monitor is not vulnerable. Can it be used
7 with some other CPU? Probably. Right? But I wouldn't say --

8 JUDGE POWELL: Let me -- let me clarify that since
9 you -- since you ask. The malicious -- the malicious attack won't
10 compromise the monitor, but it is part of a system that would be
11 compromised if attacked.

12 MR. PATHMANABAN: Yeah.

13 JUDGE POWELL: And -- and so in that situation, does
14 the term, the claim language computer system, does it -- would it
15 still read on the combination of the CPU and the monitor?

16 MR. PATHMANABAN: Yes, it would.

17 JUDGE POWELL: Okay.

18 MR. PATHMANABAN: Yes, it would.

19 JUDGE POWELL: Thank you.

20 MR. PATHMANABAN: I would say that -- that still
21 wouldn't capture Capalik's ideas because that's a completely
22 different system that nowhere is it described as part of the devices
23 to be protected or computer systems to be protected.

24 JUDGE POWELL: Thank you.

25 MR. PATHMANABAN: So let me jump to claim 2

1 quickly, Your Honors. So claim 2 requires monitoring all activity
2 on the first computer system.

3 JUDGE POWELL: What slide are we on, Counselor?

4 MR. PATHMANABAN: I'm on slide 34, Your Honor.

5 JUDGE POWELL: Thank you.

6 MR. PATHMANABAN: I want you to focus very
7 carefully on the claim language. Claim 2 does not say monitoring
8 all attack activity. It does not say monitoring all activity on the
9 virtual machine. It says monitoring all activity on the first
10 computer system. And undisputedly, the first computer system,
11 according to them, is not just the virtual machine in Capalik. It is
12 not. And this is the entirety. On the right of slide 33, I have the
13 entirety of what they said in their petition for claim 2. "As
14 explained above, Capalik features monitoring activity on the
15 computer system. See Claim [1(a)]. Capalik further features
16 monitoring all activity on the VM within the computer system."
17 That's telling. It is only monitoring activity on the VM, and there
18 is no dispute. There can be no dispute that the computer system is
19 broader than just the VM. There is also no dispute that there is
20 activity going on -- on that computer system in Capalik outside of
21 the VM. And this -- if I can jump to -- I'll just jump to slide 38
22 here just to show again this Figure 5 from Capalik, which they rely
23 on. That entire decoy computer network in green is what they map
24 to as the first computer system.

25 JUDGE POWELL: Just for the record, I think we're on

1 slide 37, correct?

2 MR. PATHMANABAN: I'm sorry. Slide 37. You are
3 right. Correct.

4 JUDGE POWELL: Thank you, Counselor.

5 MR. PATHMANABAN: So the entire decoy computer
6 is what they map to as the first computer system. They even map
7 -- remember, we had some discussion about the relational database
8 server. That's outside the VM. Clearly, there's activity going on
9 outside the VM. They have no disclosure in their petition that
10 shows monitoring in Capalik of those relational database or other
11 activities. So it fails at the outset. And even within the VM, there
12 are (INDISCERNIBLE) the operating system perform tasks
13 without user interaction. So, remember the VM -- there was a lot
14 of questions to Mr. Hart about Capalik showing when data is
15 transferred. It monitors a lot of things when data is transferred,
16 meaning when a socket connection is detected. What about
17 outside of network connections, outside of socket or port
18 connections? There's definitely activity going on in the
19 background.

20 This is their expert. We asked their expert at deposition,
21 “[d]oes the operating system perform tasks without user
22 interaction?” [Answer:] So there are background tasks that are
23 performed without a particular request from a user.” So you don't
24 need a attack for activity to be going on in a computer system, and
25 Capalik does not monitor any of that. Certainly there's no

1 disclosure in Capalik, and there's no argument in the Petition that
2 Capalik is monitoring any of that. It is no answer to say, well, the
3 disclosures in the '872 Patent and Capalik are the same. The claim
4 is talking about a first computer monitoring all activity on a
5 computer system. The claim doesn't say anything about a virtual
6 machine. We actually had a different patent, the parent patent in
7 the '872 Patent that discusses virtual machine and monitoring all
8 activity on the virtual machine. This is a claim that's requires
9 monitoring all activity on the first computer system, and they do
10 not show that in Capalik. Period.

11 JUDGE BAER: So if a machine monitors sufficiently to
12 detect and address all malicious activity but sort of ignores
13 innocuous activity, that would not meet the claim?

14 MR. PATHMANABAN: 100 percent, it would not,
15 Your Honor. It does not say. The claim does not say monitoring
16 all attacker activity or monitoring all malicious activity. It says
17 monitoring all activity. So that's a plain claim language.

18 JUDGE BAER: Okay. Thank you.

19 MR. PATHMANABAN: With that, I'll turn it over to
20 my colleague, Mr. Peters. Thank you, Your Honors.

21 MR. PETERS: Good afternoon, Your Honor. I see I
22 have five minutes left before we get into rebuttal time. Of course,
23 if Your Honors find claim 1 patentable over ground 1, that resolves
24 all disputes in this case, but I'll dive into some of the dependent
25 claims. And I'd like to start with claim 19 in slide 51. All right,

1 claim 19, Mr. Hart already showed us, depends from claim 1. It
2 recites the association includes a type. The association relates to
3 the association in claim 1, which we've already discussed, recites
4 storing in the memory a data structure that identifies, among other
5 things, the association. Now, what we see here now, claim 19
6 must require storing in the memory a data structure that identifies
7 an association that includes a type. The petition doesn't address
8 this requirement. It doesn't address the storage of a data structure
9 that identifies association that includes a type. It simply says, look
10 at Figure 3.2C. I'm now looking at slide 52. Look at Figure 3.2C.

11 There are associations here, which are the arrows, and
12 those arrows have a type. There's nothing in the petition or the
13 reply anywhere that says this data structure is stored or is the
14 stored data structure in claim 1 or claim 19. There's no argument
15 whatsoever to that effect. And in fact, what we see in King is a
16 stored event log which says: "time 0: process A creates process B,"
17 "time 1: process B writes file 1." There's no argument that there's
18 no type in that event log, right? So what we have is a combination
19 of Capalik and King. In Capalik, we have an alleged data structure
20 that identifies associations, but not associations that have a type.
21 In King, we have a type but again, no storage of a data structure
22 that identifies associations that includes type. And somehow
23 they've taken these two things and not addressed the requirement
24 that the data structure must identify this. And --

25 JUDGE POWELL: Does --

1 MR. PETERS: Now, I think they're arguing that it's
2 there somehow.

3 JUDGE POWELL: -- does the data structure itself have
4 to identify the type? Let me -- let me throw -- I'm on hypotheticals
5 again today. What if we -- what if we replaced associations with
6 sporting events and we said a data structure that lists sporting
7 events, claim 1? Claim 19 says wherein sporting events have a
8 type: football game, basketball game, baseball game. Do those
9 two claims require that I store the type of the sporting event in the
10 data structure, the football game, basketball game, et cetera? Or
11 do -- does the data structure just have to identify the sporting
12 event? Sorry for making -- taking it from the actual example, but I
13 think maybe the -- the key to my question here is: Okay, so the
14 -- the association has a type. Is that necessarily in the data
15 structure?

16 MR. PETERS: It does have to identify the association
17 that includes the type. The association includes the type, so I do
18 believe, yes, that the data structure has to also identify that type
19 that is included in the association. We see that in Figure 5A. That
20 is explicitly disclosed in the '872 Patent. The type is right there in
21 the data structure that is part of the association. What we don't
22 have in -- it's important to note that in King, not only is it, like, not
23 stored there, but it's doing extra processing in order to find a type
24 after it looks at the stored data structure, right? So it's not like
25 there is something inherent, right, or something that is known just

1 by looking process. “[P]rocess A creates process B.” What is the
2 type of that? What can we look at and say there is a type for that
3 event or what happened at time zero, right? So it's not an exact
4 analogy. Sorry, Your Honor.

5 JUDGE WHITE: But, Counselor, are we -- what are we
6 to make of the fact that claim 19 itself does not reference the data
7 structure? It just says the association includes a type. It -- it
8 doesn't say, you know, the data structure includes this type. Why
9 is that not an important distinction?

10 MR. PETERS: I don't -- I don't think it's an important
11 distinction because it is the same as if at the end of claim 1 it said,
12 wherein the association includes a type. It is read into every other
13 limitation that refers to that association. So that would include, I
14 think, 1B, which refers to identifying the association. It refers to
15 1C, which refers to the data structure that identifies the association.
16 It's -- it's going to be there as a result of dependence.

17 JUDGE WHITE: But can I not identify a thing without
18 listing all of its elements?

19 MR. PETERS: Well, we're not arguing about the
20 identification, so 1B. We're arguing about --

21 JUDGE WHITE: Is the data structure supposed to
22 identify --

23 MR. PETERS: Oh, yeah. Sorry. It has to identify an
24 association that includes a type. I think in this case the association
25 -- the type has to be identified as well.

1 JUDGE WHITE: And I think that's where we're -- why
2 does that have to be in there? When we -- when it just says that
3 there's a data structure that identifies an association.

4 MR. PETERS: Mm-hmm.

5 JUDGE WHITE: And it's in this dependent claim, the
6 association includes a type. The association could include other
7 things as well, but one of the things included in the association is
8 the type. So why does that require that the type be explicitly in the
9 data structure as opposed to any other element of the association?

10 MR. PETERS: You know, I think it has to identify the
11 association itself, and part of the association is the type. That's
12 what's being shown in 19. And -- and let's compare what you're
13 saying, though, to what is shown in King, right? In King, I think if
14 we're even going to say the as -- the stored association, at least we
15 understand it has to include a type. Whether that means there has
16 to be an explicit field that says type or not, let's set that aside.
17 What is there in the event log that includes a type? There is no
18 argument to that in this case. What is there in Capalik's forensic
19 data that includes a type? There is no argument to that in this case,
20 right? So I understand the hypotheticals about the -- the scope of
21 claim 19, but none of that has been argued by the Petitioner here.
22 All they've said is figure 3.2 C includes a type. That's not what's
23 stored. If I may, Your Honors, I need to --

24 JUDGE POWELL: So just one more time. Is it your
25 position that the -- are you conceding that the association has a

1 type, but articulating that that type is not stored? Are you
2 contesting even that the association has a type in their
3 combination?

4 MR. PETERS: Contesting that the stored association has
5 a type, yes. Including --

6 JUDGE POWELL: Well, you just changed my words
7 when you said that.

8 MR. PETERS: I know.

9 JUDGE POWELL: Are you contesting that the type
10 exists but is not stored? Are you contesting whether the type exists
11 in the first place?

12 MR. PETERS: We're contesting that it's not stored.

13 JUDGE POWELL: Thank you.

14 MR. PETERS: If I may, Your Honors, I'm into rebuttal
15 time, but I will go into claim 8 quickly on slide 45. As Mr. Hart
16 said, claim 8 depends from claim 7. Claim 7 says graphically
17 displaying at least a subset. Claim 8 says visually distinguishing at
18 least a subset of associations. Again, we're looking at Figure 3.2C
19 from King. The argument from Petitioner is that visually
20 distinguishing is the same as displaying the subset, right? So,
21 there is no dispute in this case. We look at Figure 3.2C. The rest
22 associations, the arrows, are not visually distinguished from each
23 other. They all look exactly the same. There's no bold, there's no
24 color, there's no dash lines, which are the examples provided in the
25 '872 Patent. Instead, what they're saying is they're visually

1 distinguished because there's other associations that are not shown.
2 Now, there's been some, I think, confusion generated by
3 Petitioner's arguments and by their annotations. So I'd like to look
4 at Petitioner's slide 35 -- nope, not 35. There it is. Slide 29. So
5 they've -- they've added color annotations here, and they've put
6 3.2B right next to 3.2C on slide 29 -- Petitioner slide 29. 3.2B is
7 not displayed, okay? So the -- the user is not visually able to see:
8 here's 3.2B with all of these associations, and here's 3.2C with only
9 some of them. And there's some visual distinction there by only
10 displaying on one hand some of them, on the other hand the others.
11 So that's -- this is a misleading, I think, comparison to show these.
12 The -- the user does not have that information. It's not a visual
13 distinction there. We also see in, I'll say, on slide 30 -- I didn't
14 hear Mr. Hart say it, but in their briefing -- they said King displays
15 the full 3.2B. It doesn't, right? That's on page 24 of King and
16 -- and is explained in our briefing. The last thing that I would like
17 to address, while I still have a little bit of time copying -- I'd like to
18 go to slide 55.

19 JUDGE POWELL: This is Patent Owner slide 55.

20 MR. PETERS: Patent Owner, slide 55. Yes.

21 JUDGE POWELL: Thanks.

22 MR. PETERS: Actually, 56. We have a rough outline of
23 the time -- of the timeline here, right? Dmitri Alperovitch joined
24 GoSecure's board in November 2011. A few months before that,
25 the patent application was filed, which is the parent application in

1 this case. We have direct evidence that Mr. Alperovitch was
2 exposed to that exact application in a board meeting, was exposed
3 to GoSecure's --was involved in meetings about GoSecure's
4 technology. He was a technical member of the board. He, at the
5 same time, started CrowdStrike. Three months after, I believe, in
6 this timeline, three months after he joins the board, he launches
7 CrowdStrike and starts overseeing their technology development.
8 That was his role as chief technology officer. And their only
9 product, this Falcon platform, Mr. Hart said, we don't have any
10 source code; we don't have all this. We have what they were
11 saying publicly and what they were bragging about and touting in
12 this platform. We have their video where they're describing and
13 touting their data structure, their graph database. We have
14 websites from 2013 -- this is very shortly after he left GoSecure
15 -- talking about, on slide 60, Falcon Host's highly efficient real-
16 time monitoring of all system activity is the only security solution
17 that provides maximum visibility into all adversary activities.
18 They're touting claim 2, right, as the only solution that provides the
19 best visibility. That is objective indicia of non-obviousness for
20 claim 2. We have it also for claim 1. And with that, I'll -- if
21 there's no other questions, I'll reserve the rest of my time.

22 JUDGE POWELL: When you're ready.

23 MR. HART: I'm all set.

24 JUDGE POWELL: Okay.

25 MR. HART: Thank you, Your Honor. Let me start.

1 Counsel will argue that there is no disclosure in Capalik that
2 sources, targets and associations are captured by the forensic data.
3 They argue that we had not demonstrated that in our petition,
4 essentially suggesting that the discussion of one of source, target
5 or association in fingerprint was the sum total of our discussion of
6 the content of forensic data. That is not at all accurate -- an
7 accurate depiction of what we put in our petition. Starting on page
8 25 in our petition, we discuss the output of Capalik's introspection
9 module, which is the module that generates the forensic data. We
10 describe the types of information that it monitors and what the
11 output is in the forensic data. We expressly identify sources that
12 include ports, files, instructions, data streams and any other data
13 transfers to the decoy system as express sources that are captured
14 by that forensic data generated by the introspection module.
15 Coming down to the bottom of page 25, we discuss various types
16 of target information that is also captured by the -- I'm seeing some
17 furrowed brows. Okay. Just wanted to make sure I wasn't reading
18 from the wrong document and confusing anybody. Examples of
19 target information that is also captured by the forensic data
20 generated by the introspection module. Coming down to the top of
21 page 26. A POSITA would have understood Capalik's activity
22 targets include a long list of examples. We then on page 26
23 transition to Capalik's associations, the specific types of
24 associations between targets and sources that are generated by the
25 introspection module and stored as the forensic data. This is pages

1 and pages of examples of the types of sources, targets and
2 associations that comprise the forensic data generated by Capalik's
3 introspection module and stored in the relation -- relational
4 database in Capalik's system. So the allegation that we provided
5 no details and we're just guessing as to what might be included in
6 that is absolutely wrong and not supported by the -- by the actual
7 record.

8 JUDGE BAER: In the claim language it says, "storing in
9 the memory a data structure that identifies"; assume that it had said
10 instead -- instead, storing in the memory data that is structured that
11 identifies. Are those two things meaningfully different, and does
12 Capalik have the disclosure either way? I'm trying to figure out
13 whether you're saying, look, all it needs to be is structured data
14 that in the end identifies these things, or whether there needs to be
15 stored a data structure. For example, I have to show you a table
16 that's got column headings, that sort of thing. Can you articulate
17 your position on that, whether it just needs to be any sort of
18 structured data that ends up identifying these things, or whether it
19 actually has to show a disclosure of a data structure that does these
20 things?

21 MR. HART: So, it -- it is a broader, your -- your broader
22 hypothetical example. You need to have data stored in a structure,
23 so the relational database stores the data in some mandatory
24 structure maybe imposed by that relational database. The fact that
25 we can pull that information out in a useful way to generate a

1 fingerprint tells us that it was stored, organized in some fashion to
2 make it useful.

3 JUDGE BAER: So long as it's structured data, that's
4 sufficient. Is that correct?

5 MR. HART: That -- that identifies the sources, the
6 targets, and the association for the attack that was run on that
7 virtual machine. That -- that's right, Your Honor.

8 JUDGE BAER: Thank you.

9 MR. HART: If we come to slide 21 from Patent Owner's
10 demonstratives, we see that Dr. Stavrou, Patent Owner's expert,
11 when asked, "is the forensic data produced by the introspection
12 module sufficient to teach this data structure?" "I would say the
13 information you need to create the data structure might be
14 present." So he is not disputing that the information required of
15 the data structure is missing, or he's not disputing that it's included
16 in that forensic data. This is not legitimately in dispute. The
17 dispute is all about some unclaimed arrangement of data. The data
18 that is expressly recited in the claims exists in Capalik's forensic
19 data. We spent pages and pages talking about specific examples,
20 and Dr. Stavrou agreed with us that it exists in that forensic data.
21 There was a mention of our mapping the fingerprint, where we
22 pointed only to one of source, target, and association. The
23 implication made by counsel was that we have no evidence that all
24 three exist. The reason that our mapping was framed that way is
25 because the claim requires generating information identifying one

1 or more of the activity sources, targets, or association. So this is
2 generated from that data structure. The fact that we highlighted an
3 example where there is a target does not mean that the sources and
4 associations were not also in that underlying forensic data. Patent
5 Owner's slide 21, which I just touched on. I want to be clear, and
6 we touched on this in the brief. These last two questions and
7 answers -- those were on recross. Those were leading questions
8 from Patent Owner's counsel. When I asked open-ended
9 questions, Dr. Stavrou gave me the answers that -- that we should
10 accord weight to. This cleanup process -- did you mean to ruin our
11 case by providing this clear answer to an open-ended question?
12 No. Should be accorded little weight because it is leading. Patent
13 Owner's slide 30. The ball of dough is an interesting back and
14 forth. Our expert -- I'm sorry. I'm running out of time. Our expert
15 was asked, "if you had drawn boxes differently than you actually
16 did, if your mapping that you presented us was not the same, but
17 you instead drew a box around the entire figure in Capalik, would
18 that change the operation? He spent pages and pages explaining
19 that the phrase computer system is general; it's broad; it can be
20 many things. If I take you to his actual answer here, you will see
21 that he said the lead in was: It is a general term; even the patent
22 treats this in many different ways. But if you want to map the
23 claim to the situation, the decoy -- and I'm sorry, this is Exhibit
24 2033, starting on page 58. This is the continuation of the answer
25 that you were shown by Patent Owner. The decoy computer

1 network, of course, is a computer system. It comprises one or
2 more computational devices. The protected computer network,
3 504, is another computer system. It comprises one or more
4 computational devices.

5 Now, I know from claim 1 that one computer system
6 sends information to another computer system. In the context of
7 Capalik, in Figure 5, that would correspond to the decoy computer
8 network sent 502, sending information to the computer system that
9 corresponds to the upper portion of the figure. That is the
10 protected computer network comprising the IDS, IPS, and the
11 protected endpoint devices. He was explaining exactly what the
12 mapping is. That we have narrow, targeted, and well-defined
13 computer systems, one communicating with the other, that lines up
14 precisely with the claims in this case. And I am over time. If -- if
15 you all have any questions that you would like to ask --

16 JUDGE WHITE: I have a little more. I know you're
17 over time, and we will -- we will be procedurally kind to the other
18 side. It just -- it was running a little over. With the claim 2, I
19 know it's your position that all activity is all malicious activity.
20 But what are we to make of the fact that they don't say that? The
21 claim does not say all malicious activity or all unauthorized
22 activity. It just says all activity. And if I were to go back even to
23 the claim 1 that it depends from, it says -- it says monitoring
24 activity. They've used words such as malicious, unauthorized, and
25 -- and such to describe activity that is not supposed to be

1 happening, but they don't use those words there. Why is that not
2 an issue for you?

3 MR. HART: Yes. So let me go to DX 18 where we can
4 see the full claim language for claim 1 and claim 2 here. So we are
5 a method for identifying unauthorized activities on a first computer
6 system. This is looking for attacks. Again, the entire point of the
7 disclosed invention is decoy systems running virtual machines that
8 incentivize attacks so they can be monitored. The only thing
9 monitored in the '872 Patent are attacks. The only place those
10 attacks are monitored are in those virtual machines. Now, the
11 structure of this claim is a first computer system that requires
12 processors and memory hardware. So we have to point to the
13 entire decoy system just based on the structure of this claim. If we
14 look at the intrinsic record, what is the support for what is
15 monitored?

16 It is monitoring attack activities on the virtual machine,
17 so a component of the first computer system. When we come
18 down to claim 2, where the monitoring further comprises
19 monitoring all activity on the first computer system, that is,
20 monitoring all attack activity, the only disclosure that supports
21 these claims is monitoring everything that happens in the attack as
22 that attack runs on the virtual machine as part of the entire decoy
23 system. Patent Owner addressed this briefly.

24 JUDGE WHITE: And Counsel, what does claim 2 add?
25 If claim 1 is a monitoring of activity is only going to be

1 unauthorized activity, and in claim 2 you're saying monitoring all
2 activity is monitoring all unauthorized activity, what does claim 2
3 do?

4 MR. HART: Yes. So the monitoring in claim 1 captures
5 both embodiments in the '872 Patent. I can bring you to --

6 JUDGE POWELL: I believe it's column 10.

7 MR. HART: Thank you very much. On top of it, yes, in
8 column 10, we describe, starting at line 8, in some embodiments,
9 the introspection module monitors all activity on virtualized decoy
10 operating system 112. In other environments, the introspection
11 module, instead of monitoring all activity on virtualized decoy
12 operating system 112, monitors activity on virtualized decoy
13 operating system 112 based on monitoring priority, e.g., key
14 system calls and kernel calls. So in the '872, everything that is
15 being monitored is attack activity. In some embodiments, you are
16 waiting for a trigger that some key system call has occurred before
17 you start monitoring and saving data about the sources, targets, and
18 associations. In other embodiments, as soon as that attack comes
19 in, you're monitoring everything and storing everything. That is
20 the distinction. Both those embodiments are captured by claim 1;
21 only the monitoring all activity is captured by claim 2.

22 JUDGE BAER: And I can't remember. I don't -- I don't
23 remember seeing a dependent claim that claimed the other
24 embodiment. Am -- did I miss something?

25 MR. HART: No, and I alluded to that earlier. I don't

1 believe there is a dependent claim that captures the corollary to
2 monitoring everything where it waits until it sees a key system
3 call.

4 JUDGE WHITE: Thank you.

5 MR. HART: Okay, thank you. Thank you very much,
6 Your Honors.

7 JUDGE POWELL: So we're at five and some change
8 over on Petitioner's time because we had lots of questions. I'm
9 going to be very kind and give a full six minutes to Patent Owner.

10 MR. PATHMANABAN: Thank you, Your Honor.
11 Hopefully, I won't need it, but we'll see.

12 JUDGE POWELL: Okay, here we go.

13 MR. PATHMANABAN: With respect to the petition
14 and pointing to Capalik's disclosure, all of you that -- that Mr. Hart
15 pointed to pages 25 and 26 and monitoring this data and that data,
16 all of that discussion is with -- is with respect to the monitoring
17 and identifying limitations, 1A and 1B. There is no discussion in
18 the petition with respect to 1C, which is the storing in a data
19 structure that identifies these three things, the tripartite structure
20 that's required. Capalik actually stores that information. What
21 they point to in the petition is storing forensic data. The forensic
22 data: there's no disclosure in -- in Capalik, we've talked about this
23 at length, that it is structured in the way required by the claim. As
24 for Dr. Stavrou's testimony, slide 21, the idea that he somehow
25 gave up that forensic data is a data structure is just false. You can

1 look at his testimony at length and the Q&A's. The -- the first two
2 Q&A's on slide 21 are questions and answers, the questions posed
3 by Mr. Hart, not us. And he says, "I didn't see any mention of that
4 in Capalik." What is that in reference to? He says, "logs are not
5 usually organized in the form of a data structure that clearly
6 delineates activity sources, activity targets and associations for a
7 variety of activities." "I didn't see any mention of that in Capalik."
8 And nor will Your Honors, I submit, because it's just not there.
9 With respect to their expert's testimony, I mean, it -- it says what it
10 says. I will go to slide 30. It -- he says, you can cut the dough any
11 way you want.

12 And that is essentially their claim construction, Your
13 Honors. There's no difference. There is no way, no rationale that
14 will allow them to include the IDS portion of the Capalik and
15 exclude everything else without a claim construction that would
16 essentially capture any component as part of the computer systems
17 to be protected or prevent future attacks on those computer
18 systems. As for claim 2, we can talk all we want about
19 embodiments in the '872 Patent, but this very panel has in very
20 similar circumstances with respect to the '697 patent petition that
21 they filed, they made the same argument with respect to the claim
22 language there. Obviously, there's a difference in claim language.
23 They said, you know, oh, all the disclosures in the '872 Patent are
24 -- are like Capalik, and therefore Capalik should disclose it. This
25 panel rejected it because the claim language, it doesn't matter what

1 the embodiments say or don't say. Ultimately, the claim language
2 is what counts. The claim language for claim 2 says, Monitoring
3 all activity on the first computer system. Period. End of story. It
4 doesn't say monitoring all attack activity. It doesn't say monitoring
5 all malicious activity. It doesn't say monitoring all activity on a
6 virtual machine. It says monitoring all activity, period. The end.
7 Capalik doesn't disclose monitoring all activity. That should be
8 end of story right there, Your Honors. Were there any other
9 questions I can answer for you?

10 JUDGE POWELL: None from me.

11 MR. PATHMANABAN: Thank you very much for your
12 time.

13 JUDGE POWELL: Thank you all very much for taking
14 a deep dive and --

15 JUDGE BAER: Actually.

16 JUDGE POWELL: Oh.

17 JUDGE BAER: I'm sorry. I do have an additional
18 question on secondary considerations. I didn't know --

19 MR. PATHMANABAN: Oh, I'll let my colleague
20 answer it.

21 JUDGE BAER: Yes. Sorry about that.

22 MR. PATHMANABAN: Sure.

23 JUDGE BAER: On the evidence of copying, I
24 understood all of your evidence to be about access and similarity.
25 I didn't see any additional evidence addressing things like a change

1 or anything like that. Was there anything that I missed, or was all
2 of the evidence related to access and similarity only?

3 MR. PETERS: Well, there was no change because there
4 was no company before they had access. So I-

5 JUDGE BAER: So I'm not criticizing you. I just want to
6 make sure I didn't miss anything.

7 MR. PETERS: And I just wanted to clarify, the change
8 was they started a company and created a product, right? And so,
9 yes, there was access, and then the product that they created
10 afterwards was similar.

11 JUDGE BAER: Yes. Thank you.

12 MR. PETERS: Directly similar.

13 JUDGE POWELL: Okay. As I was saying, thank you
14 for all your time today, taking a deep dive and answering our many
15 questions very well. It gives us much to think about. With that,
16 the case is submitted, and we'll -- we will go off the record. We
17 are adjourned.

18 (Whereupon, the above-entitled matter went off the
19 record at 3:08 p.m.)

IPR2025-00070
Patent 9,954,872 B2

PETITIONER:

Paul Hart
Adam Seitz
ERISE IP, P.A.
paul.hart@eriseip.com
adam.seitz@eriseip.com

PATENT OWNER:

Srinivas Giriraj Pathmanaban
Daniel Todd
Steven Peters
CLEARY GOTTlieb STEEN & HAMILTON LLP
gpathmanaban@cgsh.com
dtodd@cgsh.com
speters@cgsh.com
maofiling@cgsh.com

Raghav Bajaj
LATHAM & WATKINS LLP
raghav.bajaj@lw.com