

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-00124
Patent 9,578,045 B2

Before PATRICK M. BOUCHER, MICHELLE N. WORMMEESTER, and
AARON W. MOORE, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

CrowdStrike, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–4, 7–10, 12, and 15–18 of U.S. Patent No. 9,578,045 B2 (Ex. 1001, “the ’045 patent”). Open Text Inc. (“Patent Owner”)¹ filed a Preliminary Response (Paper 7, “Prelim. Resp.”). With our authorization, Petitioner filed a Preliminary Reply (Paper 8, “Prelim. Reply”), and Patent Owner filed a Preliminary Sur-reply (Paper 9, “Prelim. Sur-reply”).² We have authority under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we institute an *inter partes* review as to all the challenged claims of the ’045 patent based on all the grounds presented.

II. BACKGROUND

A. *Related Proceedings*

The parties identify the following four federal district court cases, one of which involves Petitioner as a defendant.

Webroot, Inc. v. Trend Micro Inc., No. 6:22-cv-00239 (W.D. Tex.);

Webroot, Inc. v. Sophos Ltd., No. 6:22-cv-00240 (W.D. Tex.);

¹ The Petition’s caption identifies Webroot Inc. as the patent owner. In Patent Owner’s mandatory notices, however, Patent Owner identifies itself, Open Text Inc., as the patent owner “due to a change in ownership of U.S. Pat. No. 9,578,045.” Paper 5, 1 n.1.

² In an e-mail dated April 5, 2023, we authorized the parties to file these papers.

Webroot, Inc. v. CrowdStrike, Inc., No. 6:22-cv-00241 (W.D. Tex.);

Webroot v. AO Kaspersky Lab., No. 6:22-cv-00243 (W.D. Tex.).

Pet. 75; Paper 5, 1 (Patent Owner’s mandatory notices).

Patent Owner additionally identifies two *inter partes* review proceedings. Paper 5, 1–2. One of these proceedings, IPR2023-00126, involves U.S. Patent No. 10,257,224 (Ex. 1010, “the ’224 patent”), which is a continuation of the ’045 patent. Paper 5, 1; Ex. 1010, code (63).

B. The ’045 Patent

The ’045 patent describes “forensic visibility into client systems having full audit trails.” Ex. 1001, 1:15–18. The ’045 patent explains that “existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic,” including hostnames, ports, protocols, and IP addresses. *Id.* at 1:34–39. The ’045 patent refers to such tools as network edge devices. *Id.* at 1:52–56. According to the ’045 patent, network edge devices “tend to receive network events outside of a host or system,” with “no ability to establish any sort of context from within the host or system that is generating the event.” *Id.* at 1:39–46. That is, a network edge device “may monitor, record, and . . . analyze network traffic between the host and the device, but information that may be useful within the host is not obtained.” *Id.* at 1:46–49. Thus, “[a] network edge device . . . has no way of knowing to what extent [a] virus may have impacted [a] computing device . . . , what additional files may have become infected, or what processes and/or objects operating are linked to the virus.” *Id.* at 2:12–16.

As a solution, the '045 patent proposes “a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event.” Ex. 1001, 2:23–27. The '045 patent describes in particular “a sensor agent [that] may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network.” *Id.* at 2:27–31. In one embodiment, “[a] computing device 204 includes and/or executes a sensor agent 208 in connection with the presentation of content to the user.” *Id.* at 7:9–11. Sensor agent 208 uses various components to gather and process events, including system filter 340, local aggregator and interpreter 344, context analyzer 348, global perspective unit 352, event distributor 356, and event priority generation unit 358. *Id.* at 7:11–17, Figs. 2, 3.

Figure 6 of the '045 patent is reproduced below.

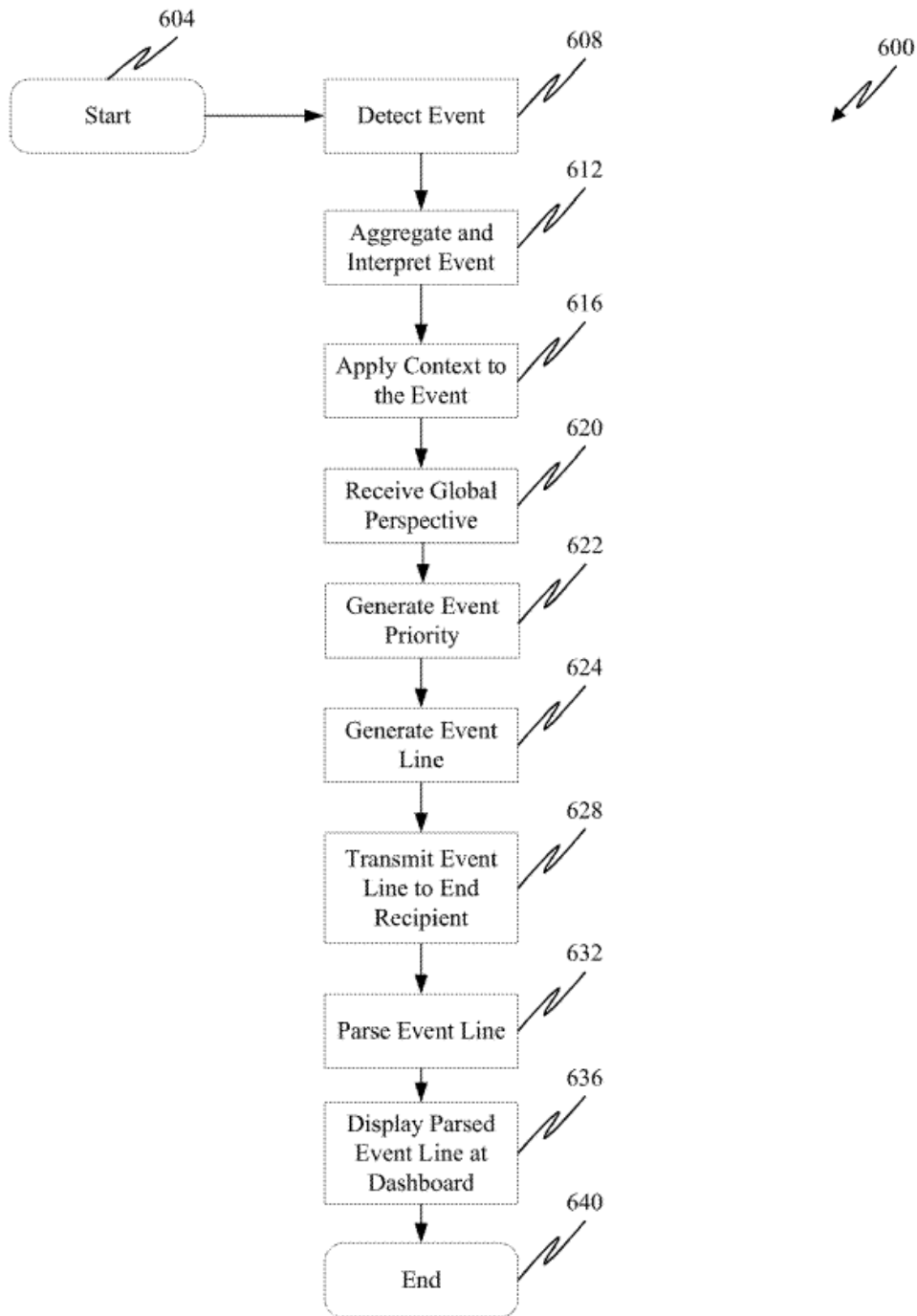


Figure 6

Figure 6 illustrates a method that sensor agent 208 may perform for providing forensic visibility into a system. Ex. 1001, 6:16–18, 18:3–7. Method 600 starts at step 604, where events of computing system 204 are

initiated. *Id.* at 18:19–21. These events are detected at step 608 by the sensor agent’s system filter 340. *Id.* at 18:21–24. At step 612, the sensor agent’s local aggregator and interpreter 344 receives the events from system filter 340. *Id.* at 18:44–47. At step 616, “a contextual state may be applied by [the sensor agent’s] context analyzer 348 to the event information,” where context analyzer 348 correlates events to objects so that an audit trail for each event is created. *Id.* at 18:53–55.

Once the contextual state is applied, “a global perspective is applied for each event and/or each object of the event and contextual state” at step 620. Ex. 1001, 18:61–63. The “global perspective” may include “information related to the age, popularity, and determination of an object—whether it is known good, bad, or unknown,” and “information pertaining specifically to an IP/URL address,” including “network activity and an assessment of the reputation and category of each website and IP address.” *Id.* at 18:64–19:5.

At step 622, “an event priority may be applied to the event,” where “the event priority may be obtained . . . [by] applying . . . a rule set to aggregated event information, contextual state information, and global perspective information.” Ex. 1001, 19:5–10. At step 624, “such data is appended to each relevant portion of an event line.” *Id.* at 19:10–12. At step 628, the sensor agent’s “event distributor 356 may transmit the event line 244 to the end recipient 220.” *Id.* at 19:13–15.

At recipient 220, the event line is parsed at step 632 to filter out one or more events, and the parsed event line is then displayed on a dashboard at step 636. Ex. 1001, 19:17–22. Method 600 ends at step 640. *Id.* at 19:22.

C. Illustrative Claim

Petitioner challenges claims 1–4, 7–10, 12, and 15–18 of the '045 patent, where claims 1, 8, and 16 are independent. Claim 1, reproduced below, is illustrative of the claims under challenge.

1. A method comprising:

gathering one or more events defining an action of a first object acting on a target;

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;

assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and

transmitting the assembled event line.

D. Asserted Grounds of Unpatentability

Petitioner challenges claims 1–4, 7–10, 12, and 15–18 of the '045 patent on the following grounds. Pet. 7–69.

Claims Challenged	35 U.S.C. § ³	References/Basis
1, 2, 4, 8–10, 12, 16	103	Morris ⁴
1–4, 8–10, 12, 16	103	Morris, van Oorschot ⁵
1, 2, 4, 7–10, 12, 15–18	103	Capalik ⁶
1–4, 7–10, 12, 15–18	103	Capalik, van Oorschot

In support of its arguments, Petitioner relies on a Declaration of Dr. Wenke Lee (Ex. 1003). *See generally* Pet.

Patent Owner relies on a Declaration of Professor Nenad Medvidovic, Ph.D. (Ex. 2001) to support its response. *See generally* Prelim. Resp.

III. DISCUSSION

A. Discretion Under 314(a)

As noted above, the '045 patent is the subject of parallel district court proceedings. *See* Part II.A. Patent Owner urges us to exercise our discretion to deny the Petition based on the state of the related litigation. Prelim. Resp. 4–19.

Under 314(a), the Director has discretion to deny institution of an *inter partes* review. *See* 35 U.S.C. § 314(a) (stating “[t]he Director *may not* authorize an *inter partes* review to be instituted unless the Director

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the application from which the '045 patent issued was filed after this date, the AIA version of § 103 applies.

⁴ Morris et al., U.S. Publ’n No. 2007/0016953 A1, published Jan. 18, 2007 (Ex. 1005).

⁵ van Oorschot et al., U.S. Patent No. 8,087,087 B1, issued Dec. 27, 2011 (Ex. 1006).

⁶ Capalik et al., U.S. Publ’n No. 2011/0321166 A1, published Dec. 29, 2011 (Ex. 1008).

determines that the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition”) (emphasis added);

Harmonic Inc. v. Avid Tech., Inc., 815 F.3d 1356, 1367 (Fed. Cir. 2016)

(“[T]he PTO is permitted, but never compelled, to institute an IPR proceeding.”). The advanced state of a parallel district court action may warrant exercising discretion on behalf of the Director to deny a petition for *inter partes* review. *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (precedential); *see also* 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”).

In determining whether to exercise such discretion, we are guided by the Director’s Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (“Interim Procedure”). As explained in the Interim Procedure, we consider the following six factors when assessing whether to use our discretion to deny institution due to the advanced state of parallel litigation:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board’s exercise of discretion, including the merits.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential). These six factors “relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Id.* at 6. In evaluating these factors, we “take[] a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.* (citing Patent Trial and Appeal Board Consolidated Trial Practice Guide 58 (Nov. 2019), <https://www.uspto.gov/TrialPracticeGuideConsolidated>).

1. Analysis of Factors

We start with an analysis of the six *Fintiv* factors, addressing each factor in turn.

a. Factor 1: Possibility of Stay

A stay of a related proceeding pending resolution of the PTAB trial “allays concerns about inefficiency and duplication of efforts.” *Fintiv* at 6. At this time, no stay has been requested or ordered in the related litigation, although Petitioner states that it “may seek a stay if institution is granted.” Pet. 69; *see also* Prelim. Resp. 5–6.

According to Patent Owner, even if Petitioner does seek a stay, it is unlikely the court will grant one because of the complexity of the related litigation, which includes multiple patents, additional defendants, and various counterclaim allegations. *See* Prelim. Resp. 6–9. Petitioner acknowledges this complexity. Pet. 71.

Even so, there has been no actual denial of a stay as contemplated by *Fintiv* to weigh this factor against exercising discretion to deny institution. Accordingly, we treat this factor as neutral. *See Fintiv* at 6–7.

b. Factor 2: Schedules

According to *Fintiv*, “[i]f the court’s trial date is earlier than the projected statutory deadline, the Board generally has weighed this fact in favor of exercising authority to deny institution.” *Fintiv* at 9. The parties agree that, according to median time-to-trial statistics in the Western District of Texas, where the related litigation is pending, the expected trial date for the related litigation is mid-July 2024. Pet. 70; Prelim. Resp. 9. This is generally consistent with the currently scheduled trial date of August 19, 2024. *See* Ex. 2007, 9 (District Court Order Granting Third Amended Scheduling Order); Prelim. Resp. 9–10. Although Petitioner contends that the complexity of the related litigation is likely to delay the trial further, the currently scheduled date is already about two months later than the deadline for the Board to issue a final written decision. *See* Pet. 71. This time difference is sufficient for this factor to weigh against exercising discretion to deny institution, and we need not speculate whether a further trial delay in the related litigation is likely.

We accordingly treat this factor as weighing against exercising our discretion to deny institution.

c. Factor 3: Investment in Parallel Proceeding

“[I]f, at the time of the institution decision, the district court has issued substantive orders related to the patent at issue in the petition, this

fact favors denial” of the Petition. *See Fintiv* at 9–10. According to the current scheduling order in the related litigation, a Markman hearing was scheduled for March 7, 2023, and fact discovery was scheduled to have opened on April 18, 2023. Ex. 2007, 3, 6. The parties have not otherwise invested a great deal in the related litigation, with fact discovery and expert discovery scheduled for closure only on January 18, 2024, and March 12, 2024, respectively. *Id.* at 7. Although Patent Owner argues that Petitioner “delayed nine months after receiving Patent Owner’s March 4, 2022 complaint, four-and-a-half months after receiving Patent Owner’s infringement contentions, and two-and-a-half months after serving its invalidity contentions before filing its petition” (Prelim. Resp. 13), such delays are not particularly long.

Patent Owner also argues under this factor that “Petitioner here has advocated for a different claim construction in the district court than in the petition,” and that the Board may “potentially issue a conflicting claim construction order.” Prelim. Resp. 12. Patent Owner claims that, “[i]n the district court, Petitioner argued that certain method steps in the challenged claims had to take place in a specific order” but that Petitioner’s challenge in this proceeding “hinges on the fact that the method steps can take place in any order.” *Id.*

We are not persuaded that this issue bears on *Fintiv* factor 3, which concerns the degree of investment, not the substance of the arguments being made. In any event, it is not unusual for a patent litigation defendant to pursue an IPR based on a broader construction (such as one offered by the patent owner) while also taking a narrower position in the district court. We find nothing inherently wrong with that and, as our rules provide, we

certainly will consider any claim construction issued by the district court and made of record. *See* 37 C.F.R. § 42.100(b).

We treat this factor as weighing against exercising our discretion to deny institution.

d. Factor 4: Overlap of Issues

“[I]f the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.” *Fintiv* at 12. Petitioner stipulates that, “if the Board institutes *inter partes* review, Petitioner will not seek resolution in the District Court of any ground of invalidity for the ’045 Patent that utilizes *Morris*, *Van Oorschot*, or *Capalik*—the prior art references relied upon in the grounds of the instant petition.” Pet. 72. This is more restrictive than a *Sand Revolution* stipulation but less restrictive than a *Sotera* stipulation. *See Sand Revolution II, LLC v. Cont’l Intermodal Grp.-Trucking LLC*, IPR2019-01393, Paper 24, 11–12 (PTAB June 16, 2020) (informative); *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 13–14 (Dec. 1, 2020) (precedential). We conclude that, while not rising to the level of a stipulation that the Interim Procedure indicates would preclude discretionary denial, Petitioner’s stipulation does mitigate concern about overlapping issues with the related litigation. *See* Interim Procedure 7–8.

We treat this factor as weighing against exercising discretion to deny institution.

e. Factor 5: Overlap of Parties

This factor weighs against exercising discretion to deny institution because, although the parties are the same as in the related litigation (*see* Pet. 73; Prelim. Resp. 15), that trial is scheduled to occur after the deadline for a final written decision in this proceeding. *See Huawei Tech. Co. v. WSOU Inv., LLC*, IPR2021-00225, Paper 11 at 14 (PTAB June 14, 2021) (stating “this factor favors denial if trial precedes the Board’s Final Written Decision and favors institution if the opposite is true”) (internal quotation marks omitted); *Google LLC v. Parus Holdings, Inc.*, IPR2020-00846, Paper 9 at 21 (PTAB Oct. 21, 2020) (“Here, . . . Petitioner is the defendant in the parallel proceeding. This fact could weigh either in favor of, or against, exercising discretion to deny institution, depending on which tribunal was likely to address the challenged patent first.”).

f. Factor 6: Other Circumstances

The final factor takes into account any other relevant circumstances, including the merits. “For example, if the merits of a ground raised in the petition seem particularly strong on the preliminary record, this fact has favored institution.” *Fintiv* at 14–15. “[C]ompelling, meritorious challenges will be allowed to proceed at the PTAB even where district court litigation is proceeding in parallel.” Interim Procedure 3–5. We address the merits of Petitioner’s challenges below. For the reasons we explain, at least some of Petitioner’s challenges meet the “reasonable likelihood” standard that we apply in determining whether to institute *inter partes* review, but do not meet the “compelling” standard. We accordingly treat this factor as neutral.

2. Balancing of Factors

As discussed above, the second, third, fourth, and fifth *Fintiv* factors weigh against exercising our discretion to deny institution; and the first and sixth factors are neutral. Given the parties' relatively modest investment thus far in the related litigation and the likelihood that trial will occur in the related litigation months after we reach a final written decision in this proceeding, we decline to exercise our discretion under 35 U.S.C. § 314(a) to deny the Petition.

B. Discretion Under 325(d)

According to Patent Owner, “[a] § 325(d) discretionary denial may be based on prior art previously considered during the prosecution of a related patent.” Prelim. Resp. 25. Patent Owner argues that “[t]he prosecution history of the ‘224 continuation patent is relevant here because its claims are similar to—and broader than—the claims in the ‘045 patent,” and “[t]he Patent Office allowed these broader claims to issue over substantively the same prior art and arguments included in the petition.” *Id.* at 26. Patent Owner argues in particular that “discretionary denial under 35 U.S.C. § 325(d) is proper because the Patent Office considered Morris 2012/0260340 (‘Morris 340’ . . .)” as well as “Capalik 2008/0016570 (‘Capalik 570’ . . .) during prosecution of the ‘224 continuation patent, which is a continuation of the ‘045 patent,” and those references are “substantively the same” as the primary references Morris and Capalik relied on in the Petition here. *Id.* at 31. Patent Owner further argues that “the Examiner explicitly considered the same argument now relied on by Petitioner in connection with an International Search Report for Morris 340

and the prior art disclosure of Kumar 2013/0298244 . . . in combination with Capalik 570” and that “[a]fter consideration of these same prior art arguments the Petition now asserts against the narrower claims of the ’045 patent, the Examiner allowed the broader claims of the ’224 continuation patent.” *Id.* Patent Owner adds that “even though the ’045 patent is earlier in time than the ’224 continuation patent, the narrower claims of the ’045 patent logically would not be unpatentable based on prior art over which the Patent Office subsequently allowed even broader claims.” *Id.* at 26–27.

Under § 325(d), we apply a two-part analysis, first assessing whether the same or substantially the same art or arguments were previously presented to the Office, and, if so, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims. *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 8 (Feb. 13, 2020) (precedential).

Becton, Dickinson & Co. v. B. Braun Melsungen AG, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017) (informative), provides a nonexclusive set of factors to use in evaluating a § 325(d) argument. Those factors are (a) the degree of similarity of the asserted art and the art involved during examination, (b) the extent to which the asserted art is cumulative; (c) the extent to which the asserted art was evaluated during examination, including whether the prior art was the basis for a rejection; (d) the extent of the overlap between the arguments made during examination and the positions taken before us; (e) whether Petitioner has sufficiently pointed out how the Examiner erred; and (f) the extent to which additional facts presented in the

Petition warrant reconsideration of the prior art or arguments. *See id.* at 17–18.

Even assuming that the prosecution history of the '224 continuation patent is relevant here, as Patent Owner contends, we decline to exercise our discretion to deny institution. We acknowledge that Morris 340 is similar to Morris, but the extent to which Morris 340 was evaluated during examination of the application for the '224 patent is unclear because it was never used in a rejection. *See generally* Ex. 2019 (file history for the '224 continuation patent). The PCT Written Opinion compared Morris 340 to the then-pending EPO claims, not the U.S. claims. And because Morris 340 was not the basis of a rejection, there is no overlap of arguments. It is not clear that there is enough similarity and overlap to move to the second step of the *Advanced Bionics* framework, but, if we did reach it, we would find, for the reasons presented in the Petition and described below, a sufficient showing that the Examiner likely erred during examination of the application for the '224 continuation patent and that the arguments presented in the Petition justify reconsideration of the '045 patent claims in view of Morris. We accordingly decline to exercise § 325(d) discretion not to institute on the grounds based on Morris.

Because, as explained below, we decide to go forward on Morris, and going forward on Morris means going forward on Capalik also, we do not reach Patent Owner's § 325(d) arguments concerning Capalik.

C. Failure to Address Secondary Considerations

Patent Owner contends that “institution should be denied” because “Patent Owner provid[ed] evidence regarding the long-felt, unmet need for

the invention and commercial success in its district court complaint against Petitioner,” and “Petitioner fails to address or consider any such evidence in its petition.” Prelim. Resp. 69 (citing Ex. 2015 ¶¶ 72–82).

In evaluating whether an invention would have been obvious, “[s]uch secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.” *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Although it is Patent Owner’s burden to introduce evidence supporting such objective indicia, *see In re Huang*, 100 F.3d 135, 139 (Fed. Cir. 1996), the ultimate burden of persuasion to prove unpatentability of the challenged claims never shifts to Patent Owner, *see Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). Rather, objective indicia should be considered along with all the other evidence in making an obviousness determination. *See Eurand, Inc. v. Mylan Pharm. Inc. (In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.)*, 676 F.3d 1063, 1076–77 (Fed. Cir. 2012) (It is “to be considered as part of all the evidence, not just when the decisionmaker remains in doubt after reviewing the art.”) (citing *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538–39 (Fed. Cir. 1983)).

We have reviewed the portions of the district court complaint that Patent Owner cites. Although Patent Owner characterizes those passages as “providing evidence” of a long-felt need, they cite only to the ’045 patent itself. *See* Ex. 2015 ¶¶ 72–82. We do not discern evidence with the kind of specificity for objective indicia of nonobviousness, notably including evidence of a nexus with the merits of the challenged claims, that would

cause us to fault Petitioner for failing to address the evidence in its Petition. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33, 31–35 (PTAB Jan. 24, 2020). We accordingly decline to deny the Petition on this basis alone.

The parties will have an opportunity during the trial to develop Patent Owner’s evidence of objective indicia of nonobviousness so that it may be fully considered.

D. Claim Construction

In an *inter partes* review proceeding, we construe a claim of a patent “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” *See* 37 C.F.R.

§ 42.100(b). That standard involves construing claims in accordance with the ordinary and customary meaning of such claims as would have been understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc).

Petitioner asserts that it “applies the ordinary and customary meaning of the claim terms as understood by a [person having ordinary skill in the art] for all terms,” except for the claim term “wherein the global perspective for one or more related events to the at least one event across a network.” Pet. 5. Petitioner further asserts, however, “[t]o limit the disputed issues, Petitioner proposes that the Board apply [Patent Owner]’s interpretation for purposes of this proceeding.” *Id.* at 6. According to Petitioner, “[Patent Owner] argued this clause . . . mandates the global perspective includes

‘information about events across the network’ and those events occur on ‘other devices’ on the network.” *Id.* at 6–7.

Patent Owner does not respond other than to assert that the district court has provided various claim constructions. Prelim. Resp. 23–25. Of relevance, Patent Owner asserts that the district court construed the claim term “wherein the global perspective for one or more related events to the at least one event across a network” to mean “wherein the global perspective [is] for one or more related events to the at least one event across [other devices on] a network.” *Id.* at 24 (citing Ex. 2008, 9 (District Court’s Claim Construction Order)).

On the record before us, at this stage of the proceeding, there does not appear to be any claim construction dispute. Accordingly, for purposes of this Decision, we conclude that no claim term requires express interpretation at this time to resolve any controversy in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

E. Morris-Based Grounds

Petitioner asserts two grounds based primarily on Morris. Specifically, Petitioner asserts that claims 1, 2, 4, 8–10, 12 and 16 of the ’045 patent would have been obvious over Morris alone. Pet. 8–37. Petitioner also asserts that claims 1–4, 8–10, 12, and 16 would have been obvious over Morris and van Oorschot. *Id.* Patent Owner challenges certain aspects of Petitioner’s analysis. Prelim. Resp. 50–56. For the reasons explained below, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing on these asserted grounds.

Before addressing the parties' arguments, we provide an overview of the asserted primary reference, Morris.

1. Overview of Morris

Morris describes a “method of classifying a computer object as malware” that includes “at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored” and “comparing in the base computer the data . . . received from the plural computers; and, classifying the computer object as malware on the basis of said comparison.” Ex. 1005 ¶¶ 14–16. The overall structure of a system according to Morris is shown in Figure 1, reproduced below.

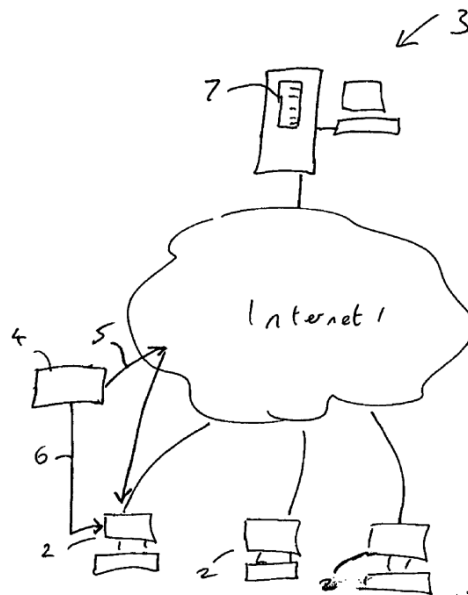


FIG. 1

Figure 1 of Morris shows a computer network based around a distributed network, such as Internet 1. *Id.* ¶ 77. Morris explains that “[p]lural local or ‘remote’ computers 2 are connected via the Internet 1 to a ‘central’ or ‘base’

computer 3.” *Id.* “An object 4 is shown schematically in the figure and may for example be downloaded to a remote computer 2 via the Internet 1 as shown by lines 5 or applied directly as shown by line 6.” *Id.* “[T]he base computer 3 holds a database 7 with which the remote computers 2 can interact when the remote computers 2 run an object 4 to determine whether the object 4 is safe or unsafe.” *Id.* ¶ 78. “The community database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2,” and “data representative of each object 4 preferably takes the form of a so-called signature or key relating to the object and its effects.” *Id.*

To illustrate how the system of Morris operates, Figure 2 of Morris is reproduced below.

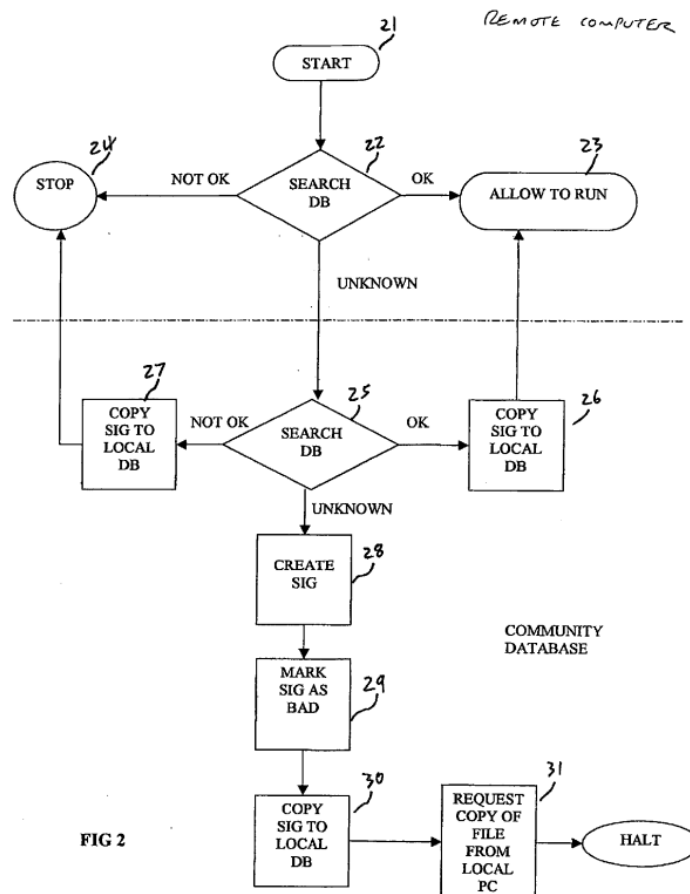


Figure 2 is a flowchart of a method according to one embodiment of Morris. Ex. 1005 ¶ 74. “[A]t the start point 21, a computer object 4 such as a process is run at a remote computer 2,” and, at step 22, “by operation of local ‘agent’ software running on the remote computer 2, the operation of the process is hooked so that the agent software can search a local database stored at the remote computer 2 to search for a signature or key representing that particular process, its related objects and/or the event.” *Id.* ¶ 79. “If the signature indicates that the process is safe, then that process or event is allowed by the local agent software on the remote computer 2 to run at step 23,” but “[i]f the signature indicates that the process is not safe, then the process or event is stopped at step 24.” *Id.*

If the object is not known locally, “then details of the object are passed over the . . . network to the base computer 3 for storing in the community database 7 and preferably for further analysis at the base computer 3.” Ex. 1005 ¶ 81. The community database 7 is searched at step 25 for a signature for the object that has already been stored in the community database 7. *See id.* If the signature is found and “indicates that that object is safe, then a copy of the signature or at least a message that the object is safe is sent to the local database of the remote computer 2 concerned at step 26 to populate the local database,” and “[a] separate message is also passed back to the remote computer 2 to allow the object to run in the current instance.” *Id.* ¶ 82. On the other hand, if the signature is found and “indicates for some reason that the object is unsafe, then again the signature is copied back to the local database and marked ‘unsafe’ at step 27, and/or a message is sent to the remote computer 2 so that running of the

object is stopped (or it is not allowed to run) and/or the user given an informed choice whether to run it or not.” *Id.* ¶ 83.

If the object is unknown, a signature is created at step 28 (or a signature sent by the remote computer 2 for this purpose is used), and the signature is initially marked as bad or unsafe by community database 7 at step 29. *See* Ex. 1005 ¶ 84. The signature is “copied to the local database of the remote computer 2 that first ran the object” and “[a] message may then be passed to the remote computer 2 to instruct the remote computer 2 not to run the object or alternatively the user may be given informed consent as to whether to allow the object to run or not.” *Id.*

If the user at the remote computer 2 chooses to run the process, “then that process may be monitored by the remote computer 2 and/or community database 7 and, if no ill effect occurs or is exhibited after a period of time of *n* days for example, it may then be considered to be safe.” Ex. 1005 ¶ 85.

Morris explains that “[t]he details of an object 4 that are passed to the base computer 3 are preferably in the form of a signature or ‘key’ that uniquely identifies the object 4.” Ex. 1005 ¶ 86. The key “is specially arranged to have at least three severable components,” one “representing executable instructions contained within or constituted by the object,” one “representing data about said object,” and one “representing the physical size of the object.” *Id.* ¶ 87.

Morris further explains that “[t]he data stored in the community database 7 provides an extensive corollary of an object’s creation, configuration, execution, behavior, identities and relationships to other objects that either act upon it or are acted upon by it” and may include “Events” (including the “Actor,” the “Event Type,” and the “Victim”);

“Identities” (which define the attributes of the object); the “Genesisactor” (“the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed”); “Ancillary data”; and “Event Checksums.” Ex. 1005 ¶¶ 96, 105–109.

2. Analysis

Turning now to the claims, we address independent claims 1, 8, and 16 in detail.

a. Independent Claim 1

Claim 1, directed to a “method,” recites various limitations designated by Petitioner as limitations 1a through 1e. We address these limitations in turn.

i. Limitation 1a: “gathering” step

Claim 1 recites “gathering one or more events defining an action of a first object acting on a target.” For this limitation, which Petitioner designates as limitation 1a, Petitioner asserts that “*Morris* discloses that ‘the base computer’ gathers ‘**events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.**’” Pet. 12 (quoting Ex. 1005 ¶ 18 (emphasis added by Petitioner)). Petitioner asserts in particular that Morris’s “[r]emote computers 2 ‘run an object 4’ and gather and transmit ‘information relating to each object run on all of the connected remote computers’ to community database 7.” *Id.* at 13 (quoting Ex. 1005 ¶ 78). Petitioner further asserts that the information is “passed over the Internet 1 . . . to the base computer 3 for

storing in the community database 7,” and that it is “passed in ‘the form of a so-called signature or key relating to the object and its effects.’” *Id.* (quoting Ex. 1005 ¶¶ 78, 81). Petitioner directs us to where Morris teaches that the key may include a component representing data about the object, such as an event. Ex. 1005 ¶ 87 (cited by Pet. 13). Morris teaches that events “define the actions or behaviours of an object acting upon another object or some other entity,” where each event has three components. *Id.* ¶ 105 (cited by Pet. 13–14). These components include the key of the object performing the act (i.e., the “Actor”), the act being performed (i.e., the “Event Type”), and the key of the object or identity of an entity on which the act is being performed (i.e., the “Victim”). *Id.*

Petitioner identifies Morris’s Actor as a “first object,” Morris’s Victim as a “target,” and Morris’s Event Type as an “action.” To illustrate, Petitioner provides an annotated version of a table in Morris, which is reproduced below. Pet. 14.

First Object	Action	Target
Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2
Object 2	Creates registry key	Object 4

The table in Morris, as annotated by Petitioner, shows various examples of the three components of an event. *See* Ex. 1005 ¶ 105.

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Morris teaches the recited gathering step of limitation 1a. Patent Owner does not

challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

ii. Limitation 1b: “generating” step

Claim 1 further recites “generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object.” For this limitation, which Petitioner designates as limitation 1b, Petitioner identifies Morris’s Genesisactor as an “originating object.” Pet. 14. As support, Petitioner directs us to where the ’045 patent teaches that “[c]ontextual state information may include, but is not limited to, originating processes, devices, and users,” as well as “GenesisActor information and ancillary data.” Ex. 1001, 8:42–45 (cited by Pet. 15). The ’045 patent describes GenesisActor information as “contain[ing] the object that is not the direct Actor of an event but which is the ultimate parent of the event being performed.” *Id.* at 8:45–48 (cited by Pet. 15).

Petitioner additionally directs us to where Morris similarly describes its Genesisactor as “the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed.” Ex. 1005 ¶ 107 (quoted by Pet. 14). Morris further describes a process that establishes whether an object is safe, unsafe, or suspicious using an object’s relationship to other objects that act on it or on which it acts. *Id.* ¶ 99 (cited by Pet. 15); *see also id.* ¶ 97. Morris teaches that “an object is considered to have a relationship based on the event performed by it upon another object, or upon it by another object,” where “[t]his simple 1-to-1 relationship chain provides a complex series of correlation points, allowing ancestral

relationships to be considered for any object and its predecessors by event or its issue (i.e. child and sub-child processes) by event.” *Id.* ¶ 99.

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Morris teaches the recited generating step of limitation 1b.

Patent Owner, however, challenges Petitioner’s analysis for this limitation. Prelim. Resp. 51–56. In particular, Patent Owner responds that “Morris does not disclose or render obvious the ‘originating object’ limitations of the claims because the ’045 patent explicitly distinguishes the GenesisActor from the claimed *originating object*.” Prelim. Resp. 53; *see also id.* (“GenesisActor information is not originating object information.”). As support, Patent Owner directs us to where the ’045 patent teaches that “[c]ontextual state information may include . . . originating processes,” and “[a]dditionally . . . may include GenesisActor information.” *Id.* (quoting Ex. 1001, 8:42–45 (emphasis added by Patent Owner)); *see also id.* at 54 (citing Ex. 1001, 17:32–38, Fig. 5B). According to Patent Owner “‘the GenesisActor is determined based on a chain of previous events’ and is an object that represents information about the *ultimate* parent of the first object.” *Id.* at 53–54 (citing Ex. 1001, 17:30–50).

Although we agree with Patent Owner that the ’045 patent distinguishes between “an origination process” and a “GenesisActor,” we do not agree with Patent Owner that the distinction means they are mutually exclusive. The current record indicates that Morris’s Genesisactor is simply the first in the chain of originating processes. *See* Ex. 1005 ¶ 107 (“Genesisactor—the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed.”). That is, it

is a species of the originating processes genus. Thus, on the present record, we conclude that the claim language “an originating object of the first object” is sufficiently broad to cover any originating object in the chain of originating objects, including Morris’s Genesisactor. Patent Owner essentially asks us to construe “an originating object of the first object” to be limited to the object that immediately originated the first object, or to exclude the first originating object, but does not actually propose, much less support, such a construction. Accordingly, Patent Owner does not adequately rebut Petitioner’s showing for the recited originating object of limitation 1b.

We note that our determination that “an originating object of the first object” reads on Morris’s Genesisactor is consistent with the PCT Written Opinion that was submitted during prosecution of the related ’224 patent. *See* Ex. 2019, 270 (stating that “the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]”).

iii. Limitation 1bi: “contextual state”

In connection with the recited generating step of limitation 1b, claim 1 recites “the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object.” Petitioner designates this limitation as limitation 1bi. Pet. 16. According to Petitioner, “[t]his limitation recites a disjunctive list of alternatives,” and, therefore, “Petitioner must only show the prior art discloses one of the recited options of the Markush group.” *Id.* at 16 n.3. With respect to obviousness over

Morris alone, Petitioner focuses primarily on “an indication of . . . a device on which the first object is executed.” *See* Pet. 17–18.

In particular, Petitioner provides another annotated version of the table in Morris, which is reproduced below. Pet. 17.

Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2
Object 2	Creates registry key	Object 4

Morris’s table, as annotated by Petitioner, shows various examples of the three components of an event. *See* Ex. 1005 ¶ 105. The second event in the annotated table is highlighted in yellow. Pet. 17. Petitioner asserts that Morris’s “‘**Genesisactor**’ teaches the claimed *contextual state including an indication of the originating object of the first object.*” *Id.* at 16. Petitioner asserts in particular that, as “the ‘ultimate parent of the [second] event being performed’—such as the file that created ‘Object 1’ (i.e., the *first object*),” Morris’s “‘Genesisactor’ would indicate *the originating object of the first object.*” *Id.* at 16–17. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* (citing Ex. 1003 ¶ 88).

Petitioner also asserts that “*Morris* discloses the contextual state can further include *an indication of . . . a device on which the first object is executed*, boxed in red . . . as ‘**IP Address 3.**’” Pet. 17. As support, Petitioner states that “*Morris* discloses the ‘Victim’ is the ‘identity of another entity upon which the act is being performed,’” and, therefore, “the first object, ‘Object 1,’ is executed on the device identified as ‘IP Address 3’

in that data is sent to this device.” *Id.* Petitioner relies on the declaration testimony of Dr. Lee. *Id.* (citing Ex. 1003 ¶ 89).

We note that Petitioner also argues that, “[t]o the extent Patent Owner argues *Morris* does not disclose *an indication of at least one of a device on which the first object is executed [or] a user associated with the first object*, [v]an Oorschot discloses a similar computer security system that captures event data,” including “the user initiating the event” and “the system or device on which the event occurred,” and that an ordinarily skilled artisan “would have understood these as disclosing the claimed *device on which the first object is executed and a user associated with the first object*.” Pet. 18 (citing Ex. 1006, 6:14–23). Petitioner contends that “[i]t would have been obvious . . . to modify *Morris*’s system to capture additional types of event data, such as the ‘device on which the event occurred’ and the ‘user initiating the event’ as disclosed by [v]an Oorschot” because “[i]t was a common principle in the art of computer security systems that gathering more detailed information from threats results in improved threat analysis and detection.” *Id.* at 19. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* at 18–20 (citing Ex. 1003 ¶¶ 93–98).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that *Morris* teaches the recited contextual state of limitation 1bi. We also are persuaded that Petitioner has shown sufficiently for purposes of this Decision that its proposed combination of *Morris* and van Oorschot teaches the recited contextual state of limitation 1bi. Additionally, we are persuaded that Petitioner’s proffered reasoning for modifying *Morris* to capture event data regarding the device on which the event occurred and the user initiating the

event as taught by van Oorschot is sufficient for institution. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (“[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”). Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

iv. Limitation 1c: “obtaining” step

Claim 1 further recites,

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information.

Petitioner designates this limitation as limitation 1c. Pet. 20. As with limitation 1bi, Petitioner asserts that “[t]his limitation recites a Markush group.” *Id.* at 20 n.4. Accordingly, Petitioner addresses “the information including . . . Internet Protocol (IP) Address,” “information including . . . a determination as to whether the first object is malware,” “information including . . . a determination as to whether the originating object is malware,” and “information including . . . popularity.”

With respect to information including Internet Protocol (IP) Address, Petitioner cross-references its analysis for limitation 1bi and asserts that “*Morris* discloses obtaining the IP Address of the device where the first object is executed.” Pet. 20. Petitioner additionally refers again to the second event in *Morris*’s table (*see* Ex. 1005 ¶ 105), reiterating that “the first object, ‘Object 1,’ sends data to the device identified as ‘**IP Address 3.**’”

Id. According to Petitioner, “[t]he IP Address of the device Object 1 (i.e., *first object*) sends data to therefore constitutes information *associated with the first object*,” and, “[t]hus, *Morris* discloses the claimed *obtaining a global perspective for the at least one event by obtaining information associated with . . . the first object . . . the information including at least . . . Internet Protocol (IP Address)*.” *Id.* at 20–21.

With respect to information including a determination as to whether the first object is malware and information including a determination as to whether the originating object is malware, Petitioner asserts that “*Morris* discloses after event data and associated contextual metadata is gathered and generated, this data is sent to base computer 3,” which “compares ‘the data about the computer object received from the plural computers’ and **‘classif[ies] the computer object as malware on the basis of said comparison.’**” Pet. 21 (citing Ex. 1005 ¶¶ 14–17, 20, 78). Petitioner further asserts that “[t]his comparison involves identifying ‘relationships between the object and other objects’ to ‘immediately and automatically [] **mark a child object as bad** (or good) [] **or a parent or other related object [a]s bad** (or good).” *Id.* (citing Ex. 1005 ¶¶ 19, 96). According to Petitioner, “*Morris* therefore discloses obtaining a global perspective for the event by obtaining information concerning *a determination as to whether the first object/originating object is malware*.” *Id.* at 22.

With respect to information including popularity, Petitioner asserts that “*Morris* also discloses a heuristic used ‘to establish if an object is safe, unsafe or suspicious,’ involving analyzing ‘time and **volumes**.’” Pet. 22 (citing Ex. 1005 ¶¶ 97–101). Petitioner asserts that “this heuristic obtains information concerning ‘**how many times [the object] has been seen**, how

many times it has been seen in a given interval of time, and the increase or decrease of acceleration in it being seen.” *Id.* (citing Ex. 1005 ¶ 101). Petitioner further directs us to where the ’045 patent states that, “[f]or unknown files, the dashboard may show their popularity at the global community, i.e. on how many computing systems 204 they have been seen.” *Id.* (quoting Ex. 1001, 16:15–18). According to Petitioner, “[t]herefore, *Morris* discloses obtaining a global perspective for the event with information concerning the *popularity* of the first object in the same way as the ’045 Patent.” *Id.*

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that *Morris* teaches the recited obtaining step of limitation 1c. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

v. Limitation 1ci: “global perspective”

In connection with the recited obtaining step of limitation 1c, claim 1 further recites “wherein the global perspective for one or more related events to the at least one event across a network.” For this limitation, which Petitioner designates as limitation 1ci, Petitioner asserts that it “applies [Patent Owner]’s interpretation of this limitation—that the global perspective includes ‘information about events across the network’ and those events occur on ‘other devices’ on the network.” Pet. 22. We note that the district court’s construction of limitation 1ci (i.e., “wherein the global perspective [is] for one or more related events to the at least one event across

[other devices on] a network”) appears to be consistent with this interpretation. *See* Prelim. Resp. 24; Ex. 2008, 9.

As Petitioner states, “*Morris*’s method ‘comprises connecting the computer to a community database that is connectable to a plurality of computers, and **uploading the stored data to the community database for comparison with similar data provided by other computers.**’” Pet. 22–23 (quoting Ex. 1005 ¶ 67 (emphasis added by Petitioner)). Petitioner directs us to where Morris explains that “[t]his aspect allows a comparison to be made between the objects and/or their effects on the different remote computers **to determine whether or not a particular object should be classed as good or as malware.**” *Id.* at 23 (quoting Ex. 1005 ¶ 17 (emphasis added by Petitioner)). According to Petitioner, “*Morris* therefore discloses that a global perspective includes information from other related events across the network, such that a malware determination takes into account object events on other devices.” *Id.*

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Morris teaches the recited global perspective of limitation 1ci. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

vi. Limitation 1d: “assembling” step

Claim 1 further recites “assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object.” For this limitation, which Petitioner designates

as limitation 1d, Petitioner asserts that Morris’s “[r]emote computers 2 ‘run an object 4’ and gather and transmit ‘information relating to each object run on all of the connected remote computers’ to community database 7” of base computer 3. Pet. 24 (quoting Ex. 1005 ¶ 78). Petitioner directs us to where Morris teaches that such information “takes the form of a so-called signature or key relating to the object and its effects,” where the “key may be formed by a hashing function operating on the object at the remote computer 2.” Ex. 1005 ¶¶ 78, 86 (cited by Pet. 24). Petitioner also directs us to where Morris teaches that the key may include information about events, such as “the key of the object performing the act (the ‘**Actor**’), the act being performed (the ‘**Event Type**’), and the key of the object or identity of another entity upon which the act is being performed (the ‘**Victim**’),” as well as the “**Genesisactor**.” *Id.* ¶¶ 18, 78, 105, 107 (cited by Pet. 24); *see also id.* ¶ 87 (cited by Ex. 1003 ¶ 115). According to Petitioner, Morris therefore “discloses *assembling an event line including details associated with the at least one event (key) the details including information uniquely identifying the first object (Actor) the action of the first object (Event Type) the target (Victim) and the originating object (Genesisactor)*.” Pet. 24. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* (citing Ex. 1003 ¶¶ 114–116).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Morris teaches the recited assembling step of limitation 1d. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

vii. Limitation 1e: “transmitting” step

Lastly, claim 1 recites “transmitting the assembled event line.” For this limitation, which Petitioner designates as limitation 1e, Petitioner cross-references its analysis for limitation 1d and asserts that “*Morris* discloses transmitting its key to base computer 3 for processing.” Pet. 24. In its analysis for limitation 1d, Petitioner directs us to where *Morris* describes “the data about the computer object that is sent from the plural remote computers to the base computer,” where the data “takes the form of a so-called signature or key relating to the object and its effects.” Ex. 1005 ¶¶ 18, 78 (cited by Pet. 24). Petitioner adds, “*Morris* also discloses this key can be subsequently ‘copied to’ the local database of a remote computer that first ran the object.” Pet. 24–25 (citing Ex. 1005 ¶ 84).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that *Morris* teaches the recited transmitting step of limitation 1e. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

b. Independent Claim 8

Independent claim 8 is directed to a “system for providing forensic visibility into a system,” which corresponds to the “method” recited in claim 1. Except for limitations that correspond to the different statutory classes, Petitioner relies on its analysis of claim 1. *See* Pet. 30–32. Patent Owner makes no separate arguments for claim 8, relying instead on the same analysis as for claim 1. *See* Prelim. Resp. 50–56. Our analysis for claim 1 applies to claim 8.

c. Independent Claim 16

Independent claim 16 also is directed to a “system for providing forensic visibility into a system,” which corresponds for the most part to the “method” recited in claim 1. Petitioner relies largely on its analysis for claims 1 and 8. *See* Pet. 35–37. Our analysis for claim 1 applies to claim 16.

Unlike claim 1, claim 16 requires that the recited “event line” further include “global perspective information comprising information about one or more related events to the one or more events across a network.” For this limitation, Petitioner asserts that “*Morris* discloses assembling a key (i.e., *event line*) comprising information identifying the first object, action of the first object, target, and originating object and transmitting this key to a base computer for analysis,” which “includes determining an IP address associated with the first/originating object, determining if the first object and/or originating object is malware, and determining a popularity associated with these objects (i.e., *global perspective information comprising information about one or more related events to the one or more events across a network*).” Pet. 36 (cross-referencing analysis for claim 1). In addition, Petitioner asserts that “*Morris* discloses its key at the base computer can then be ‘copied to’ the local database of the remote computer that first ran the object.” *Id.* (citing Ex. 1005 ¶ 84). According to Petitioner, an ordinarily skilled artisan “would have understood [that] this key copied back to the remote computer would include the same event information above, including the IP address of the Victim (i.e., the global perspective).” *Id.* Petitioner contends that “[i]t would have been obvious to a [person having ordinary skill in the art] to store the malware determinations in this

key as well to better inform a user regarding the significance of the event on the computing system.” *Id.* at 36–37. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* at 36–37 (citing Ex. 1003 ¶¶ 157–158).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Morris teaches the recited event line of claim 16. Patent Owner makes no separate arguments for claim 16, relying instead on the same analysis as for claim 1. *See* Prelim. Resp. 50–56.

3. Summary

In view of the foregoing, we determine that Petitioner has demonstrated a reasonable likelihood of showing that independent claims 1, 8, and 16 would have been obvious over Morris alone as well as over Petitioner’s proposed combination of Morris and van Oorschot. Claims 2–4, 9, 10, and 12 depend from claims 1 or 8. Having reviewed Petitioner’s arguments asserting that claims 2, 4, 9, 10, and 12 would have been obvious over Morris alone as well as Petitioner’s arguments asserting that claims 2–4, 9, 10, and 12 would have been obvious over Morris in combination with van Oorschot, (*see* Pet. 25–30, 32–35), we also determine that Petitioner has demonstrated a reasonable likelihood of prevailing on its assertions as to these dependent claims.

F. Capalik-Based Grounds

Petitioner asserts two grounds based primarily on Capalik. Specifically, Petitioner asserts that claims 1, 2, 4, 7–10, 12, and 15–18 of the ’045 patent would have been obvious over Capalik alone. Pet. 37–69.

Petitioner also asserts that claims 1–4, 7–10, 12, and 15–18 would have been obvious over Capalik and van Oorschot. *Id.* Patent Owner challenges certain aspects of Petitioner’s analysis. Prelim. Resp. 57–68. For the reasons explained below, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on these asserted grounds.

Before addressing the parties’ arguments, we provide an overview of the asserted primary reference, Capalik.

1. Overview of Capalik

Capalik describes “systems and methods for analyzing malicious activities on a computer system.” Ex. 1008 ¶4. In the method, “[a] plurality of activities performed at a virtual machine is identified,” where “[e]ach of the activities includes an activity source, an activity target, and an association between the activity source and the activity target.” *Id.* ¶ 10. Then, “[a] fingerprint indicative of the activity on the virtual machine is created from the stored activities” and “transmitted to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.” *Id.* Capalik describes producing the fingerprints using a “decoy network device” that runs one or more virtual machines running “decoy operating systems.” *See id.* ¶¶ 33–48.

2. Analysis

Independent claims 1 and 8 recite “wherein the global perspective for one or more related events to the at least one event across a network.” We refer to this limitation as the network limitation. Independent claim 16

similarly recites “global perspective information comprising information about one or more related events to the one or more events across a network.” Petitioner indicates that it “assumes [the network] limitation requires the global perspective to include information about events across the network and that those events occur on ‘other devices’ on the network.” Pet. 50.

In that regard, Petitioner argues that Capalik teaches that its methods “need not be restricted to analysis of a single virtualized operating system, but, rather, **are able to follow a chain of unauthorized activity across multiple virtualized operating systems**.” Pet. 50 (citing Ex. 1008 ¶ 130). Petitioner contends that an ordinarily skilled artisan “would have understood that in an attack across multiple virtualized operating systems, *Capalik’s* methods would follow the related chain of unauthorized activity across each operating system and would perform the methods identified . . . for obtaining a global perspective—namely, identifying an activity source and the activity target (e.g., by ‘an Internet Protocol address’) and determining ‘association types’ between sources and targets, including ‘malicious associations.’” *Id.* at 50–51. According to Petitioner, in this way, “*Capalik’s* disclosed methods include obtaining a global perspective which includes information about events across a network, including obtaining an IP Address for the first object or a malware determination for the first object or originating object.” *Id.* at 51. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* at 50–51 (citing Ex. 1003 ¶¶ 186–187).

Petitioner also provides an annotated version of Figure 4E of Capalik, reproduced below. Pet. 52.

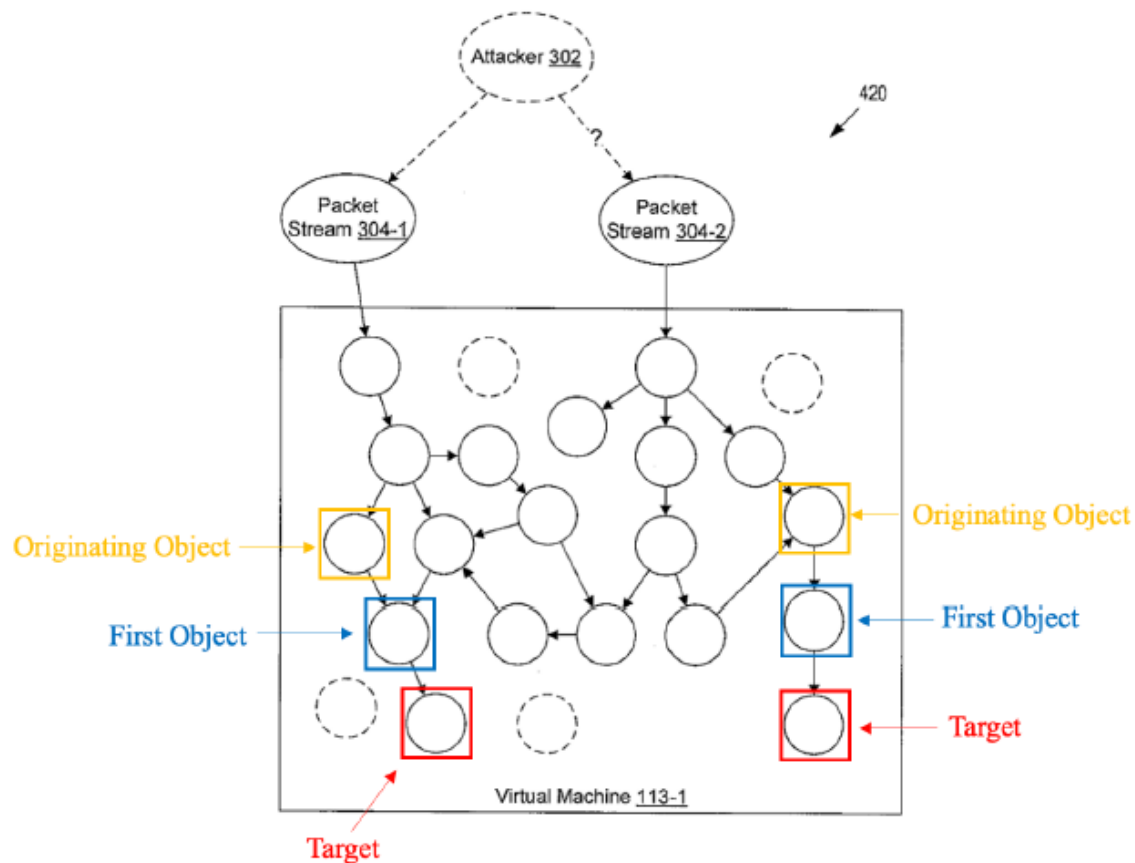


Figure 4E

Capalik's Figure 4E, as annotated by Petitioner, shows network diagram 420 of unauthorized activities on a computer system, namely, virtual machine 113-1. *See* Ex. 1008 ¶¶ 19, 74. Petitioner contends that the annotated figure shows specifically how "*Capalik's* methods include obtaining the 'Internet Protocol address' of the device where the first objects are executed and making a malware determination for the originating and/or first objects." Pet. 52. Petitioner relies on the declaration testimony of Dr. Lee. *Id.* (citing Ex. 1003 ¶ 189).

Petitioner additionally argues that, "[t]o the extent [Patent Owner] argues *Capalik's* multiple virtualized operating systems are in a single device, a [person having ordinary skill in the art] would have understood

Capalik's system is scalable and would have been motivated to implement multiple virtualized operating systems not only within a single device, but also across a plurality of decoy network devices to protect network devices 136-n as contemplated by *Capalik*.” Pet. 51 (citing Ex. 1008 ¶ 30).

Petitioner asserts that “it was known in the art to accumulate information from several attacked devices to inform a malware determination,” and that “when an attack spreads across multiple systems (i.e., multiple decoy network devices), the associated activity chain would be tracked and a malware determination would be made based on the monitored information.” *Id.* Petitioner relies on the declaration testimony of Dr. Lee. *Id.* (citing Ex. 1003 ¶ 188).

Patent Owner counters that “while *Capalik* teaches that its method is ‘able to follow a chain of unauthorized activity across multiple virtualized operating systems,’ these virtualized operating systems reside on the same single decoy network device,” which “is not capable of performing this [network] limitation because the global perspective cannot ‘relate[] to one or more other events related to the event ***across a network***.”” Prelim. Resp. 62–63 (citing Ex. 1008 ¶¶ 45–46). Regarding *Capalik's* Figure 4E, Patent Owner asserts that “the events Petitioner cites all occur on one virtual machine (and one decoy network device) and ***not across a network***.” *Id.* at 63. Patent Owner relies on the declaration testimony of Dr. Medvidovic. *Id.* at 60–64 (citing Ex. 2001 ¶¶ 64, 66, 71–76).

With respect to Petitioner’s argument that *Capalik's* system is scalable, Patent Owner responds that, “[e]ven if one were to utilize multiple decoy network devices, Petitioner fails to identify any *Capalik* teaching or embodiment that includes sharing information across decoy computer

network devices.” Prelim. Resp. 66. According to Patent Owner, “Capalik does not teach transmitting . . . information between decoy network devices, or the use of this information from multiple decoy network devices to create a fingerprint.” *Id.* at 67. Patent Owner relies on the declaration testimony of Dr. Medvidovic. *Id.* at 65–67 (citing Ex. 2001 ¶ 75).

We find that Petitioner has not shown how the network limitation is met in Capalik. The discussion of this limitation in the Petition relies on general statements in Capalik that its methods “are able to follow a chain of unauthorized activity across multiple virtualized operating systems” and enable “identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems,” but we fail to see how that teaches or suggests the recited limitation “wherein the global perspective for one or more related events to the at least one event across a network,” which, according to Petitioner, requires a showing of “information about events across the network and that those events occur on ‘other devices’ on the network.” *See* Pet. 50. Petitioner does not explain how an ability to follow unauthorized activity relates to the claimed global perspective, and the cited language discusses tracking activity across multiple “operating systems,” not across a network.

Capalik’s Figures 6A–6C provide an overview of its method, showing that it generally works by monitoring activity on a virtual machine (step 602); identifying activities, including their source, target, and association (step 604); identifying an association as malicious (step 610); and identifying sources that are affected by unauthorized activities (step 614). *See* Ex. 1008 ¶¶ 100–108. The method determines an activity status and an activity level (steps 632 and 634) and creates a fingerprint indicative of the

activity on the virtual machine (step 636). *See id.* ¶¶ 116–120. Then, “[t]he decoy network device transmits ([step] 644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.” *Id.* ¶ 126.

For the claimed global perspective, Petitioner points to Capalik’s determination of whether the objects are malware using the data structure of Figure 5A, corresponding to step 610. *See Pet.* 48–50. But nothing in the description of that step indicates that any of the information used relates to an event related to the event across a network. *See Ex.* 1008 ¶¶ 75–96, 106. Instead, Capalik describes determining that activity is malicious if it performs unauthorized activities on the decoy network device, not because it is related to another event across a network. *See id.* ¶ 106 (“By identifying that the process A 308 performed unauthorized activities, the process A 308 is determined to be affected by the unauthorized activities, and the association between the socket 306 and the process A 308 is determined to be malicious (i.e., unauthorized).”).

With respect to Figure 4E, as Patent Owner observes, the objects and targets all exist within one virtual machine (113–1). Petitioner does not explain how that teaches or suggests obtaining a global perspective that relates to one or more other events related to the event “across a network.”

As to Petitioner’s scalability argument, Petitioner does not explain sufficiently why an ordinarily skilled artisan would have considered modifying Capalik’s system to provide a “global perspective for one or more related events to the at least one event across a network,” which, according to Petitioner, requires a showing of “information about events across the network and that those events occur on ‘other devices’ on the network.” *See*

Pet. 50. As Petitioner correctly observes, Capalik contemplates a decoy computer network with “one or more decoy network device(s) 106.”

Ex. 1008 ¶ 30 (cited by Pet. 51). Capalik explains, however, “[t]he purpose of the decoy network device 106 is to allow attackers to attack the decoy network device 106, so that the pattern of the attack can be monitored and analyzed to generate a fingerprint,” which “can be used to prevent similar attacks on the decoy network device 106 and/or other computers (e.g., protected network devices 136).” *Id.* Petitioner does not explain why an ordinarily skilled artisan would have considered modifying Capalik’s system “to accumulate information from several attacked devices to inform a malware determination,” (*see* Pet. 51), when Capalik’s system already accumulates information from its decoy network device 106 to inform a malware determination, (*see* Ex. 1008 ¶ 30).

On the record before us, we are not persuaded that Petitioner has shown sufficiently for purposes of this Decision that Capalik teaches or suggests the recited “one or more related events to the at least one event across a network” of claims 1 and 8, or the similarly recited “one or more related events to the one or more events across a network” of claim 16. Nor are we persuaded that Petitioner has sufficiently shown why an ordinarily skilled artisan would have considered modifying Capalik’s system to provide these limitations. We note that Petitioner’s reliance on van Oorschot does not cure this deficiency. *See* Pet. 46–47 (relying on van Oorschot for the limitation “an indication of at least one of a device on which the first object is executed and a user associated with the first object”).

3. *Summary*

In view of the foregoing, we determine that Petitioner has not demonstrated a reasonable likelihood of showing that independent claims 1, 8, and 16 would have been obvious over Capalik alone or in combination with van Oorschot. Because claims 2–4, 7, 9, 10, 12, 15, 17, and 18 depend from claims 1, 8, or 16, we also determine that Petitioner has not demonstrated a reasonable likelihood of showing that these dependent claims would have been obvious over Capalik alone or in combination with van Oorschot.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated on the record before us a reasonable likelihood that it will prevail in showing at least one of the challenged claims of the '045 patent is unpatentable. We institute trial on all challenged claims and all asserted grounds of unpatentability. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1353 (2018) (“The agency cannot curate the claims at issue but must decide them all.”); 37 C.F.R. § 42.108(a) (“When instituting . . . review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”). We have not, however, made a final determination with respect to the patentability of the challenged claims.

V. ORDER

For the reasons given, it is

ORDERED that *inter partes* review is instituted as to all challenged claims of the '045 patent, namely, claims 1–4, 7–10, 12, and 15–18, based on all grounds presented in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this Decision.

PETITIONER:

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

PATENT OWNER:

Brian Eutermoser
Russell E. Blythe
Mikaela Stone
KING & SPALDING LLP
beutermoser@kslaw.com
rblythe@kslaw.com
mikaela.stone@kslaw.com