

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AO KASPERSKY LAB,
Petitioner, v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-01334
Patent 8,418,250 B2

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

LIST OF EXHIBITS

Exhibit 1001	U.S. Patent No. 8,418,250 to Morris et al. ("250 Patent")
Exhibit 1002	File History of U.S. Patent No. 8,418,250 ("250 File History")
Exhibit 1003	Declaration of Dr. Wenke Lee ("Decl.")
Exhibit 1004	U.S. Patent Application Publication No. 2005/0210035 A1 to Kester et al. ("Kester")
Exhibit 1005	U.S. Patent No. 7,225,343 to Honig et al. ("Honig")
Exhibit 1006	U.S. Patent No. 7,594,272 to Kennedy et al. ("Kennedy")
Exhibit 1007	Plaintiff's Opposition Markman Brief, 22-cv-00243 WDTX, No. 98
Exhibit 1008	Intentionally left blank
Exhibit 1009	Intentionally left blank
Exhibit 1010	Defendants' Opening Markman Brief, 22-cv-00243 WDTX, No. 86
Exhibit 1011	<i>Intrusion Detection with Unlabeled Data Using Clustering</i> by Leonid Portnoy, et al. ("Portnoy")
Exhibit 1012	U.S. Patent No. 6,944,772 to Dozortsev ("Dozortsev")
Exhibit 1013	U.S. Patent No. 6,772,363 to Chess et al. ("Chess")
Exhibit 1014	WO 2002/033525 to Shyne-Song Chuang
Exhibit 1015	EP 1,549,012 to Kristof De Spiegeleer
Exhibit 1016	EP 1,280,040 to Alexander James Hinchliffe, et al.
Exhibit 1017	U.S. Patent Publication No. 2004/0153644 to McCorkendale ("McCorkendale")
Exhibit 1018	U.S. Patent No. 7,516,476 to Kraemer ("Kraemer")
Exhibit 1019	Harold S. Javitz et al., <i>The NIDES Statistical Component: Description and Justification</i> ("The NIDES Statistical Component: Description and Justification")
Exhibit 1020	U.S. Patent No. 7,448,084 to Apap et al.
Exhibit 1021	Order Granting Third Amended Scheduling Order, 22-cv-00243 WDTX, No. 142 ("Third Amended Scheduling Order")
Exhibit 1022	Declaration of V.S. Subrahmanian, Ph.D.
Exhibit 1023	Order Granting Fifth Amended Scheduling Order, ECF No. 252, Mar. 29, 2023

TABLE OF CONTENTS

LIST OF EXHIBITS	i
TABLE OF CONTENTS	ii
I. INTRODUCTION	1
II. KESTER IS ANALOGOUS TO THE ‘250 PATENT AND HONIG.....	1
A. Kester Is Analogous To The ‘250 Patent.....	1
i. Kester is in a relevant field of endeavor	2
ii. Even if Kester is not within the field of the inventor’s endeavor, Kester is reasonably pertinent to the problem faced by the inventor of the ‘250 patent	3
B. Kester And Honig Are Analogous	6
i. Kester/’250 patent and Honig are all in the relevant field of endeavor, namely, classifying and controlling specific software objects.	7
ii. Kester/’250 are also reasonably pertinent to the problem faced by Honig.....	7
III. THE CLAIMS DO NOT REQUIRE THE “MASK TO DEFINE ONLY ACCEPTABLE BEHAVIOR FOR THE OBJECT” AND KESTER RENDERS THIS LIMITATION OBVIOUS	8
A. Patent Owner’s Construction Of “Mask That Defines Acceptable Behavior For The Object” Is Improper.....	8
B. Ground 1 Renders Obvious “Mask That Defines Acceptable Behavior For The Object”	10
IV. GROUND 1 RENDERS OBVIOUS “AUTOMATICALLY GENERATING A MASK”	17
V. GROUND 1 RENDERS DEPENDENT CLAIMS OBVIOUS	22
A. Cited combination renders obvious claims 7 and 19.....	22
B. Cited combination renders obvious claims 12 and 24.....	23
C. Cited combination renders obvious claims 2, 9-11, 14, 19, 21-23, 27-30	25
VI. GROUND 2 RENDERS OBVIOUS CHALLENGED CLAIMS	25

VII. CONCLUSION	25
CERTIFICATION UNDER 37 CFR § 42.24(d)	27
CERTIFICATE OF SERVICE	28

I. INTRODUCTION

Patent Owner's Patent Owner Response ("POR") relies on improper claim constructions and flawed reasoning to elide the actual disclosures of the references. Indeed, Patent Owner ("PO") incorrectly concludes that the Kester reference is nonanalogous to the '250 patent, and further that the Honig reference is nonanalogous to the Kester patent.

For these reasons, the Board should find the Challenged Claims of the '250 patent unpatentable.

II. KESTER IS ANALOGOUS TO THE '250 PATENT AND HONIG

A. Kester Is Analogous To The '250 Patent

For a reference to be proper for use in an obviousness rejection under 35 U.S.C. 103, the art reference must be analogous to the claimed invention. *In re Bigio*, 381 F.3d 1320, 1325, 72 USPQ2d 1209, 1212 (Fed. Cir. 2004). A reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). *Id.* It should also be noted that the "same field of endeavor" and "reasonably pertinent" are two alternative tests for establishing analogous art; it is not necessary for a reference to

fulfill both tests in order to qualify as analogous art. *Id.* Kester and the '250 patent are both in the relevant field of endeavor, namely, classifying and controlling specific software objects.

i. Kester is in a relevant field of endeavor

When determining whether the “relevant field of endeavor” test is met, one should consider “explanations of the invention’s subject matter in the patent application, *including the embodiments, function, and structure* of the claimed invention.” *Airbus S.A.S v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019) (emphasis added) (quoting *Bigio*, 381 F.3d at 1325). Furthermore, the primary focus is on what the reference discloses. *Airbus*, 41 F.3d at 1380. The disclosure of each reference must be considered “in view of the ‘the reality of the circumstances.’” *Id.* at 1380 (quoting *Bigio*, 381 F.3d at 1326). These circumstances are to be weighed “from the vantage point of *the common sense* likely to be exerted by one of ordinary skill in the art in assessing the scope of the endeavor.” *Id.* (emphasis added) (internal quotations omitted); *See also Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353 (Fed. Cir. 2020).

The PO spends much energy describing the various functions and analysis that Kester can carry out, while minimizing the plain fact that Kester and the '250 patent are both in the same field of endeavor of classifying and controlling specific software objects. *See gen.* POR; Ex. 1003, ¶ 62. In fact, the PO goes on to state that a feature

of the Kester reference is that it does indeed identify and control a category of “malicious applets and scripts,” thus admitting that Kester and the ‘250 patent both analyze and classify computer objects as “malicious applets or scripts,” or “malware.” Ex. 1004, Fig. 4A, [0082]. This one fact, in and of itself, is sufficient to show that Kester is in the same field of endeavor as the ‘250 patent and is therefore analogous.

ii. Even if Kester is not within the field of the inventor's endeavor, Kester is reasonably pertinent to the problem faced by the inventor of the ‘250 patent

A prior art reference that is not within the field of the inventor's endeavor may still be analogous if it is reasonably pertinent to the problem faced by the inventor. The problem faced by the inventor should be considered, as reflected in the specification, either explicitly or implicitly. *See In re ICON Health and Fitness*, 496 F.3d 1374, 1379-80 (Fed. Cir. 2007). For a reference to be “reasonably pertinent” to the problem, it must “logically [] have commended itself to an inventor's attention in considering his problem.” *Id.* (internal quotations omitted) (quoting *In re Clay*, 966 F.2d 656, 658 (Fed. Cir. 1992)); *See also In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011). An inventor is not reasonably expected to have been aware of all prior art outside of the field of endeavor. *Airbus*, 41 F.3d at 1380-82. A reference outside of the field of endeavor is reasonably pertinent if a person of ordinary skill would have consulted it and applied its teachings when faced with the problem that the

inventor was trying to solve. *Id.* “[T]he reasonably [] pertinent inquiry may consider where an ordinarily skilled artisan would reasonably look, and what that person would reasonably search for, in seeking to address the problem confronted by the inventor.” *Airbus*, 941 F.3d 1382–83. The question of whether a reference is reasonably pertinent often turns on how the problem to be solved is perceived. In conducting the “reasonably pertinent” analysis, the problem cannot be viewed in such a narrow way that would be inconsistent with the specification – such a technique would inappropriately limit with scope of available prior art. *See e.g. Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359, (Fed. Cir. 2020) (“Thus, when addressing whether a reference is analogous art with respect to the claimed invention under a reasonable-pertinence theory, the problems to which both relate must be identified and compared.”).

In this case, Kester is reasonably pertinent to the problem faced by the inventor of the ‘250 patent. The inventor of the ‘250 patent sought to address the problem of classifying and controlling specific software objects, including identification of inadequate malware detection software. Specifically, conventional anti-malware software employed human analysts to perform a deep analysis on new objects such that a database of signatures (e.g., a hash or checksum) is manually updated to identify known malware. Ex. 1001, 1:18-2:64. This introduced both delay

and risk. Ex. 1001, 2:57-64. Likewise, Kester seeks to identify malware, to initially classify an object as not malware, to generate a mask for the object that defines acceptable behavior for the object, and to reclassify the object if the actual monitored behavior is not normal (extending beyond the mask). *Compare* Ex. 1001, 4:21-30, 15:2-4, *with* Ex. 1004, [0076] (describing an application that is “not operating in a predetermined manner [is] categorized or re-categorized”), [0179]-[0181], Claims 1-2; Ex. 1003, ¶¶57-63. Both the ‘250 patent and Kester address the same central problem – identification of malware. Consequently, it is reasonable to conclude that an ordinarily skilled artisan would reasonably look to references such as Kester for its disclosure of malware identification and classification.

PO incorrectly classifies the problem addressed by the ‘250 patent as exceedingly narrow. Particularly, PO argues that the only problem the ‘250 patent sought to remedy was the time-consuming nature of malware detection and eradication. POR, 27-30. This argument is PO's attempt to show that inventor could not have referenced Kester. However, PO neglects to recognize that the central problem addressed by both the ‘250 patent and Kester is classifying and controlling specific software objects, which includes the identification and classification of malware.

PO similarly assigns an inadequately narrow definition of the problem

addressed in Kester. PO argues that “Kester is concerned with allowing a company to implement policies to control what programs and network access their employees can make on their computers.” POR, 112. While this may be one aspect of the problem addressed in Kester, this neglects Kester's main purpose: to address the problem of classifying and controlling specific software objects. Ex. 1004, [0005]. Contrary to PO's argument that a “POSITA would not have looked to Kester in considering these problems,” Kester includes categories that are closely related to software security; therefore, a POSITA would likely consider the disclosures in Kester when addressing this problem. POR, 26.

B. Kester And Honig Are Analogous

The PO also argues that the Honig reference suffers from the same apparent deficiencies of Kester. Specifically, these alleged deficiencies include failure to disclose automatically generating a mask or a mask that defines acceptable behavior. PO attempts to advance the idea that Honig is not capable of automatically generating a mask, nor a mask that defines acceptable behavior. For the reasons described below, this argument is categorically false.

As also set forth above, Kester is analogous to the '250 patent, as Kester and the '250 patent are in the same field of endeavor and reasonably pertinent to the same problem. Honig is analogous to Kester/'250 patent as Honig also is in the same

field of endeavor and is reasonably pertinent to the same problem.

i. Kester/'250 patent and Honig are all in the relevant field of endeavor, namely, classifying and controlling specific software objects.

As described above in greater detail, the relevant field of endeavor for Kester/'250 is classifying and controlling specific software objects. Likewise, Honig falls into this field of endeavor, as it teaches a method and system for **classifying applications** as normal or anomalous. Ex. 1005, 15:43-16:24 (describing an automated process to classify suspicious activity as “either anomalous” (i.e. malware) or normal); *see also* Ex. 1005, 8:14-18 (describing classifying activity as either “malicious or normal”); Ex. 1003, ¶¶64-66. Therefore, Honig is analogous to Kester/'250.

ii. Kester/'250 are also reasonably pertinent to the problem faced by Honig.

Furthermore, Kester/'250 is reasonably pertinent to the problem faced by Honig, and vice versa. Specifically, Honig is reasonably pertinent to certain problems addressed by Kester/'250, such as the need to classify the object as anomalous if the actual monitored behavior is not normal (extending beyond the mask). *Compare* Ex. 1001, 4:21-30, 15:2-4, Claims 1, 13, 25, *with* Ex. 1005, 8:15-18 (“The data in the data warehouse 14 is accessed by the detection model generators 16 which generate models that classify activity as either malicious or normal”), 24:43-45 (“The model generator 16 then uses the unsupervised SVM algorithm to

generate a model of normal activity.”); *see also* Ex. 1005, 4:54-57 (“What is needed is an architecture to automate the processes of . . . model generation . . . and to solve many of the practical problems associated with the deployment of data mining-based IDSs.”); Ex. 1003, ¶¶64-66. Therefore, Honig is analogous art to Kester.

III. THE CLAIMS DO NOT REQUIRE THE “MASK TO DEFINE ONLY ACCEPTABLE BEHAVIOR FOR THE OBJECT” AND KESTER RENDERS THIS LIMITATION OBVIOUS

A. Patent Owner's Construction Of “Mask That Defines Acceptable Behavior For The Object” Is Improper

Patent owner asks the Board to interpret “mask that defines acceptable behavior for the object” as “a mask that defines *only* acceptable object behavior” POR, 33 (emphasis added). Conversely, in the associated litigation, PO argued no construction was necessary other than “plain and ordinary meaning.” POR, 12. As recognized by PO, the district court “construed the term to have its plain and ordinary meaning, while specifically explaining that ‘the plain-and-ordinary meaning of this term is *not the inverse of a mask of unacceptable behavior.*’” POR, 13 (emphasis added) (quoting Ex. 2012, 4). A mask that defines *only* acceptable behavior is not the same as “the inverse of a mask of unacceptable behavior.” The former provides that the only definitions allowed by the mask are definitions of acceptable behavior. The latter provides that acceptable behavior is whatever is not defined as

unacceptable behavior.

Adding such language to Claims 1, 13, and 25 is improper and represents an impermissible attempt to amend the claim language without the proper procedure of a motion to amend. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (“[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment.”). Any motion to amend must comply with the content requirements of 37 C.F.R. §§ 42.121(b) or 42.221(b).

Additionally, Patent Owner has not satisfied the stringent requirements associated with a disclaimer of claim scope. “To disavow claim scope, the specification must contain ‘expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.’” *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1306 (Fed. Cir. 2011) (quoting *Epistar Corp. v. Int’l Trade Comm’n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009)). Rather than citing to the specification to support this disavowment of claim scope, PO cites to Petitioner CrowdStrike’s arguments made during claim construction, where Petitioner CrowdStrike argued for a construction of “a list of acceptable actions for the object to perform,” not for PO’s proposed construction of mask that defines **only** acceptable behavior. Here, at best, the specification provides for what type of behavior a mask

may include or define but does not teach what a mask cannot include or define. As stated in the Petition, “the ’250 Patent discloses a mask that ‘can be built up with use of that object, . . . can give an overall picture of the expected “normal” behavior of that object,’ and might indicate ‘details of any ports or interfaces’” for legitimate Internet connections. Ex. 1001, 14:55-58, 15:2-4. Accordingly, a POSITA would have understood Kester teaches generating a mask for the computer object that defines acceptable behavior for the object, wherein the mask is generated in accordance with normal behavior of the object determined from said received data. Ex. 1003, ¶¶117-120; Petition, 29.

This and Patent Owner's other attempts to improperly limit the scope of the Challenged Claims are unsupported by the law, unsupported by the district court's claim construction in the ongoing litigation and should be rejected.

B. Ground 1 Renders Obvious “Mask That Defines Acceptable Behavior For The Object”

As set forth in the Petition, Kester teaches “its application categorization and classification process includes determining an application's “**expected or allowed network activity**” (i.e., *generating a mask*). See Ex. 1004, [0179]-[0181], Fig. 20; *see also* Ex. 1004, [0070] (“expected network access data is derived from network access data obtained when the application is behaving in a predetermined manner”);

Petition, 28; *see also* Ex. 1003 ¶117.

PO contends that Kester does not teach a “mask that defines acceptable behavior for the object” because “the hash/policy table and the expected network activity identified within that table includes unacceptable behavior.” POR, 32-33, (citing Ex. 1004 [0070], [0185]). Therefore, PO does not dispute that Kester's teaches a “mask” or that Kester's “mask” defines acceptable behavior as claimed by the '250 patent. Rather, PO appears to argue that a mask that includes unacceptable behavior cannot also teach a mask that defines acceptable behavior because it “includes unacceptable behavior.” POR, 32-33

However, this is not what claim 1, 13, and 25 recite. Rather, the claims require a “mask that defines acceptable behavior.” As stated above, there is no restriction in the claim language or the specification identifying what the mask does not define. Similarly, none of the additional limitations cited by PO in claims 1, 13, and 25 mandate limiting a mask to what it does not define. A mask that defines both acceptable and unacceptable behavior, can still allow, disallow, or reclassify based on whether the monitored behavior is within the definition of acceptable or outside of the definition of acceptable. As stated in the petition and by Dr. Lee, in Kester, “a human reviewer (at the application server module 102 and/or application database factory 110) interacts with a classification user interface to *determine the ‘expected*

or allowed network activity' (also referred to as expected or predetermined behavior) for an application from, for example, a record of the 'application's prior activity' or contemporaneous activity on one or multiple workstations." Petition, 28-29 (emphasis added); Ex. 1004, [0179]-[0181]; *see also* Ex. 1003 ¶117.

Even if the Board agrees with PO's construction of a "mask that defines acceptable behavior" Kester teaches this limitation. None of the arguments provided by PO support the assertion that Kester's mask "includes unacceptable behavior." POR, 32-33.

First, a significant portion of PO's arguments in this section are directed to whether Kester's approach is similar to the '250 approach, the benefits of "automatically" generated masks and whether Kester relies on human review. *See* POR, 33-35. These arguments are not pertinent to whether Kester teaches a mask that defines acceptable behavior.

PO argues that Kester teaches a mask that includes unacceptable behavior in several ways; however, as demonstrated in the Petition, PO misinterprets and misconstrues Kester's teachings. PO argues that Kester teaches a mask that includes unacceptable behavior because "when an application is not operating in a 'predetermined manner,' it is placed in the uncategorized applications database for future review, such that those attributes might be added to the hash/policy table."

POR, 33, (citing Ex. 1004 [0070]). PO further asserts that this means “whether an application is operating in a ‘predetermined’ or ‘expected’ manner is dependent on whether that activity is contained within the hash/policy table *and not whether that activity is acceptable or unacceptable.*” POR, 33.

It is unclear how behavior being “predetermined” or “expected” does not also mean that the behavior is acceptable. It is also unclear how placing an application into a database for further review when not operating in a predetermined/expected manner, (i.e. allowed manner) means that the mask includes unacceptable behavior. PO does not further expand upon this conclusory statement and the Expert declaration (para 126) is just as conclusory.

As stated in the Petition and by Dr. Lee in his declaration, “Kester teaches its application categorization and classification process includes determining an application’s ‘**expected or allowed network activity**’ (i.e., *generating a mask*).” Petition, 28 (citing Ex. 1004, [0179]-[0181], Fig. 20, [0070] (“expected network access data is derived from network access data obtained when the application is behaving in a predetermined manner”)); Ex. 1003 ¶117. Accordingly, the determination of whether an application is operating in a “predetermined” or “expected” manner depends on the matching of its behavior characteristics, i.e., “properties or features” listed in the table entry. Ex. 1004, [0070].

PO further argues that Petitioner has wrongly equated “‘expected’ network activity with ‘allowed network activity’ because ‘an application operating in an expected or predetermined manner’—*i.e.*, within the boundaries of Petitioner’s alleged ‘mask’—might still be disallowed from continuing to run, based on the associated policy.” POR, 36-37 (citing Ex. 2019 ¶¶124-126). PO concludes this argument by stating that “Kester relies on a hash/policy table containing “expected” activity reviewed by a human administrator that may include acceptable activity but that also includes unacceptable activity.” POR, 38. PO further supports this argument with an example of how even if activity is “expected,” depending on the specific workstation attributes associated with the “expected behavior,” the behavior and specific workstation may be associated with a policy that does not allow the behavior on that specific workstation. POR, 37-38.

It is unclear how a mask that is capable of distinguishing acceptable object behavior on a workstation-by-workstation basis means that the mask must also include disallowed behavior rather than simply defining allowed behavior for the workstation and anything outside of the allowed behavior for the workstation is outside of the allowed behavior and therefore disallowed, similar to the claims of the ‘250 Patent. As taught by Kester, “[n]ext, at a state 2004, the application analyst's classification module 302 is utilized to display the application and any related data

on the GUI. The related data can indicate to the human reviewer the expected network activity for the application. As explained above, the application analyst classification module 302 allows the human reviewer to analyze each application and any additional data that is associated with the application to determine an expected or allowed network activity.” Ex. 1004, [0179]. As further stated by Dr. Lee, “[o]nce determined, the expected or allowed network activity of the application is *stored in the hash/policy table* by the workstation management module, in the master application database of the application database factory, and *in the application inventory database of the application server module.*” Ex. 1003, ¶118 (internal citations omitted) (emphasis added).

Dr. Lee also discusses that, “Kester’s expected network activity includes one or more network attributes, also referred to as properties or features, that are associated with the application when the application accesses the network in an expected (*normal*) manner. The attributes can include a specific protocol, IP address and/or port.” Ex. 1003, ¶119 (citing Ex. 1004, [0046]). Accordingly, as indicated by PO, “because ‘network attributes associated with the application may be different for each attempted access,’ its system ‘may allow a first combination of one or more network attributes while disallowing a second combination of the one or more network attributes.’” POR, 36 (quoting Ex. 1004, [0185], [0083]). PO attempts to

assert that because one combination is allowed and another is not allowed that Kester's "mask" includes definitions of disallowed behavior. However, as stated by Dr. Lee, "[a] skilled artisan would have understood that determining the 'expected network activity' based on prior or contemporaneous network activity, as taught by *Kester*, teaches *generating a mask for the program/application that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the application/program determined from said received data.*" Ex. 1003, ¶120 (emphasis added). As stated in the petition:

Kester teaches "denying access to the network" (*disallowing the computer object to run*) when the network accessing application properties/attributes (*the actual monitored behavior of the computer object*) do not match an expected behavior for the application (*extends beyond that permitted by the mask*). *Kester*, [0055], [0059], [0145].

For example, expected network activity (as listed in the hash/policy table 204 of each remote workstation) includes "attributes [that] are associated with the application when the application accesses the network in an expected manner" (e.g., a specific protocol, a specific IP address, and a specific access port). *Kester*, [0184]. According to *Kester*, "[i]f the application requests access to the network using a different protocol than the expected protocol listed in the hash/policy table 204, the network access detection module 208 may disallow access." *Id.*

Petition, 35-36. The disallowed “second combination” is simply behavior that “extends beyond that permitted by the mask” as described in the claims of the ‘250 patent. Ex. 1001, Claim 1.

PO provides what it terms “another example” of how Kester does not teach “a mask that defines acceptable behavior” by stating that “because Kester’s expected network activity defines unacceptable behavior, it cannot be used as a tool for informing when an application must be reclassified as malware.” POR, 40. However, whether Kester’s mask can be used as a tool for information when an application must be reclassified as malware is inapplicable to whether Kester’s teaches a “mask that defines acceptable behavior.” PO did not assert in its response that Kester does not disclose “reclassifying the computer object as malware when the actual monitored behavior extends beyond that permitted by the mask.” And, therefore, this example is inapplicable and moot.

Accordingly, as stated above, in the Petition, and by Dr. Lee, Ground 1 renders obvious a “mask that defines acceptable behavior for the object.”

IV. GROUND 1 RENDERS OBVIOUS “AUTOMATICALLY GENERATING A MASK”

The PO argues that both Kester and Honig fail to disclose automatically generating a mask or a mask that defines acceptable behavior. Specifically, PO

forces the argument by stating that “Kester does not “automatically” generate a mask because a human is actively involved throughout Kester’s entire process.” POR, 42. Further, PO argues that Honig in combination with Kester does not disclose automatic mask generation because Honig’s adaptive learning model that is limited to a binary decision and cannot be combined with Kester’s determination of expected network activity. POR, 48-52. Without further explanation, PO states that “even if a POSITA were to combine Kester’s and Honig’s teachings, the resulting combination still does not render obvious a mask that defines acceptable behavior.” POR, 3. Petitioner disagrees.

As stated in the Petition, “Kester teaches its application categorization and classification process includes determining an application’s ‘**expected or allowed network activity**’ (i.e., *generating a mask*) Although Kester does not explicitly state the mask is generated ‘automatically,’ such an implementation would have been obvious based on the teachings of Kester in view of Honig.” Petition, 28 (quoting Ex. 1004, [0179]-[0181]). As further explained in the Petition, “[w]hile Kester’s mask generation involves human input, Kester explains the process for classifying or categorizing applications ‘can be based upon [] adaptive learning systems[.]’” Petition, 29-30 (quoting Ex. 1004, [0089], [0092]). As further explained by Dr. Lee and in the petition “[a] POSITA would have found it obvious to look to

known adaptive learning systems to perform Kester's classification and/or categorization processes. [] As described above [in the Petition], Honig teaches a known process for generating adaptive learning models to inform malware determinations/classifications." Petition, 30 (citing Ex. 1004, [0179]-[0181]). Accordingly, while Kester may not teach "automatically generating a mask," it does provide motivation to look to adaptive learning systems for combination, contrary to PO's argument that a POSITA would not be motivated to automate Kester's determination of expected network activity. POR, 47-48.

PO does not appear to dispute that Honig teaches automatedly generating a mask. Instead, PO argues a POSITA would not be motivated to combine Honig with Kester. PO argues that Honig's "binary classifier" cannot be used to automate Kester's determination of expected network activity without "extensive ongoing modifications." POR, 48-50. PO further argues that a POSITA would not be motivated to automate Kester with Honig because such automation would undermine Kester's stated goal of "managing employees' interactions with the internet." POR, 52-53. Finally, PO argues in general that Petitioner failed to provide sufficient motivation to combine Kester and Honig. POR, 55-58. However, none of PO's arguments arise to a teaching away or a lack of motivation to combine.

“A party that petitions the Board for a determination of obviousness must show that ‘a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” *Apotex Inc. v. Wyeth LLC*, IPR2014-00115, Paper 94, slip op. at 11 (Apr. 20, 2015) (quoting *Procter & Gamble Co. v. Teva Pharms. USA, Inc.*, 566 F.3d 989, 994 (Fed. Cir. 2009)). “A reason to combine may be found explicitly or implicitly in market forces; design incentives; the interrelated teachings of multiple patents; any need or problem known in the field of endeavor at the time of invention and addressed by the patent; and the background knowledge, creativity, and common sense of the person of ordinary skill.” *Ericsson, Inc. v. Intellectual Ventures I LLC*, IPR2014-00527, Paper 41, slip op. at 27–28 (May 18, 2015) (internal quotations omitted).

As stated in the Petition and by Dr. Lee, “[a]s part of Honig’s techniques, Honig discloses a model generator 16 that automatically generates a model of normal behavior for a computer object This model of normal behavior can then be used to make a malware determination/classification.” Petition, 30; *see also*, Ex. 1003, ¶¶123-124.

As further stated by Dr. Lee, “a skilled artisan would have been motivated to generate *Kester’s* ‘expected or allowed network activity’ (i.e., *mask*) for an

application using an adaptive learning model as disclosed in *Honig* because it is expressly contemplated by *Kester*.” Ex. 1003, ¶125 (citing Ex. 1004, [0089], [0092], Fig. 20 [0090]). Dr. Lee further states that:

[a] skilled artisan would have been familiar with adaptive learning systems as of 2005 in the context of intrusion and malware detection systems and would have understood that such systems require no human input. A skilled artisan considering the teaching of *Kester* that generation of the mask can be based upon ‘adaptive learning systems’ would have found it obvious to generate the mask automatically (e.g., without any human decisions) with any of the well-known and readily available adaptive learning systems—such as *Honig*’s readily available adaptive learning system.

Ex. 1003, ¶125. As further stated in the Petition and by Dr. Lee:

[a] POSITA would have recognized automating mask generation to be an obvious and predictable improvement to *Kester*’s server module and/or database factory classification software, given that *Kester* expressly contemplates use of adaptive learning systems. Ex. 1003, ¶¶121-131. Moreover, *Honig* recognized the need for an extensible and scalable system where the model generator components are modular components that are “plugged” into the system architecture...this modification would have been well within the capabilities of a POSITA such that there would have been a reasonable expectation of success.

Petition, 31-32; see also Ex 1003, ¶¶121-131.

Accordingly, as stated above, in the Petition, and by Dr. Lee, Kester in view of Honig renders obvious automatically generating a mask and a POSITA would have been motivated to combine Honig with Kester.

V. GROUND 1 RENDERS DEPENDENT CLAIMS OBVIOUS

A. Cited combination renders obvious claims 7 and 19

PO argues that the combination of Kester and Honig render obvious “*wherein the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers,*” because “[n]one of the cited evidence, nor the declaration of Dr. Lee, shows that Kester’s remote computers carry out a hashing process on the collection data...” POR, 59. However, as stated by Dr. Lee, “*Kester* explains that the application related data (*see* element 1.1 [of the Petition] and claim 2) may be sent in the form of a hash (i.e., *key*) that is generated by each remote workstation using a hash function. *Kester*, [0051] (“As part of its analysis, the execution launch detection module 210 can **generate a hash** for the application using the application digest generator 201. The application digest generator 201 **parses properties** from the requested application to uniquely identify the application. These properties can include net-work access data. Exemplary properties include the name, publisher, suite, hash, file size, version, protocol, I.P. address, port, and additional information or properties which are associated with a

launched or network accessing application”). Ex. 1003, ¶152 (*bolding added*).

Accordingly, as stated above, in the petition, and by Dr. Lee, the cited combination renders obvious claims 7 and 19.

B. Cited combination renders obvious claims 12 and 24

PO argues that the combination of Kester and Honig do not teach “*allowing behavior for the object if said behavior is known to be not malicious for other objects,*” because instead of comparing the activity-in-question with known activity of other objects to determine whether the activity-in-question should be allowed, Kester will immediately permit or not permit access based on the default ‘not classified’ policy. POR, 60-61. This argument by PO appears to read into the claim limitation **immediately** “*allowing behavior for the object if said behavior is known to be not malicious for other objects.*” However, no such additional language appears in the claims.

As stated by Dr. Lee, Kester explains “that an application that is ‘not operating in a predetermined manner [is] categorized or re-categorized’ and that ‘[t]he application is re-categorized based on parsed properties or features which are different than the parsed properties or features associated with the original categorization of the application.’ *Kester*, [0076]. Thus, in my opinion, *Kester* teaches comparing at the base computer the non-permitted behaviour (e.g., ‘the parsed properties or features that are different’) with the behaviour of other objects

(e.g., ‘the parsed properties or features associated with the original categorization of the application’). Ex. 1003, ¶164. Dr. Lee further goes on to state that “categorization and re-categorization can include categorizing/re-categorizing the expected or allowed network activity for the application.” Ex. 1003, ¶166.

Further, PO does not appear to dispute that Honig teaches “*allowing behavior for the object if said behavior is known to be not malicious for other objects*,” but instead argues that “Petitioner does not address the deficiency in Kester or explain why a POSITA would have modified Kester to delay applying its “not classified” policy....” POR, 61. Again, this argument appears to read into the claim limitation **immediately** “*allowing behavior for the object if said behavior is known to be not malicious for other objects*” and also implies an ordering to the limitations of the independent claims. This additional language and ordering is not required or even implied by the claim language.

Further, the Petition does provide motivation to combine Honig with Kester to render obvious claims 12 and 24. As stated in the Petition and by Dr. Lee, “[a]s noted above, *Kester*’s disclosures already contemplate such an implementation, but do not detail how this implementation would work. A PHOSITA would have been motivated to apply the teachings of *Honig* to ensure when unexpected behavior actually represents normal operation, *Kester*’s expected network activity is modified

accordingly, thereby reducing false alarms and nuisance to *Kester's* employee end users. This implementation would have made *Kester's* method/system more desirable and more effective in identifying malicious/rogue programs (malware), thereby improving similar malware detection method/systems in the same way.”
Petition, 46-47 (citations removed).

Accordingly, as stated above, in the Petition, and by Dr. Lee the combination renders obvious claims 12 and 24.

C. Cited combination renders obvious claims 2, 9-11, 14, 19, 21-23, 27-30

For the reasons stated in the petition, by Dr. Lee, and as addressed above the combination renders obvious claims 2, 9-11, 14, 19, 21-23, and 27-30.

VI. GROUND 2 RENDERS OBVIOUS CHALLENGED CLAIMS

For the reasons stated in the petition, by Dr. Lee, and as addressed above, Ground 2 renders obvious the challenged claims.

VII. CONCLUSION

For these reasons, the Board should find the challenged claims of the ‘250 Patent to be unpatentable.

Respectfully submitted,

Dated: February 22, 2024

/s/ Joseph T. Miotke

Joseph T. Miotke, Reg. No. 47,798

Eric H. Chadwick, Reg. No. 41,664

IPR2023-00289
Patent No. 8,418,250
Petitioner's Reply to Patent Owner's Response

Erin Block, Reg. No. 78,154
DeWitt LLP
901 Marquette Avenue
Suite 2100
Minneapolis, MN 55042
T: (612) 305-1400
F: (612) 305-1414
jtm@dewittllp.com;
ehc@dewittllp.com;
eblock@dewittllp.com;
docketing@dewittllp.com

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petitioner Reply to Patent Owner Response to Petition totals 5,557, which is allowed under 37 CFR § 42.24(c)(1).

Respectfully submitted,

Date: February 22, 2024

/s/ Joseph T. Miotke

Joseph T. Miotke, Reg. No. 47,798
Eric H. Chadwick, Reg. No. 41,664
Erin Block, Reg. No. 78,154
DeWitt LLP
901 Marquette Avenue
Suite 2100
Minneapolis, MN 55042
T: (612) 305-1400
F: (612) 305-1414
jtm@dewittllp.com;
ehc@dewittllp.com;
eblock@dewittllp.com;
docketing@dewittllp.com

CERTIFICATE OF SERVICE

Pursuant to 37 CFR § 42.6(e)(4), the undersigned certifies that on February 22, 2024, a complete and entire copy of this Petitioner Reply to Patent Owner Response and supporting exhibits were provided via email, to the Patent Owner by serving the email correspondence address of record as follows:

Brian Eutermoser, Reg. No. 64,058
Russell E. Blythe, Reg. No. 58,440
Mikaela Stone, Reg. No. 70,404

KING & SPALDING LLP
1401 Lawrence Street,
Suite 1900
Denver, CO 80202

Email: beutermoser@kslaw.com
Email: rblythe@kslaw.com
Email: Mikaela.stone@kslaw.com

/s/ Rachel Gagliardi
Rachel Gagliardi
DeWitt LLP
901 Marquette Avenue
Suite 2100
Minneapolis, MN 55042