Trials@uspto.gov
571–272–7822

Paper 37
Entered: February 16, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2021-01150
Patent 10,530,903 B2

Before STACEY G. WHITE, JON M. JURGOVAN, and AARON W. MOORE, *Administrative Patent Judges*.

WHITE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Palo Alto Networks, Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review of claims 1–18 of U.S. Patent No. 10,530,903 B2 (Ex. 1001, "the '903 patent"). We instituted an *inter partes* review of the challenged claims on all asserted grounds. Paper 9 ("Dec."). After institution, Centripetal Networks[1], Inc. ("Patent Owner") filed a Patent Owner Response (Paper 19, "PO Resp."), Petitioner filed a Reply (Paper 23, "Reply"), and Patent Owner filed a Sur-Reply (Paper 26). An oral hearing was held on October 31, 2022, and a transcript of the hearing is included in the record (Paper 34, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons that follow, we determine Petitioner has not shown by a preponderance of the evidence that claims 1–18 are unpatentable.

A. *Related Proceedings*

The parties indicate that the '903 patent is the subject of the following co-pending district court case: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, No. 2:21-cv-00137 (E.D. Va.). Paper 33, 1; Paper 3, 1. Petitioner informs us that the district court case has been stayed pending the resolution of this proceeding. Paper 12, 1.

B. *The '903 Patent*

The '903 patent discloses methods and systems for "correlating packets in communications networks." Ex. 1001, 1:38–39. Figure 1,

[1] On January 19, 2023, Patent Owner notified the Board of a change in corporate name to Centripetal Networks, LLC. *See* Paper 35.

reproduced below with added coloring, shows the architecture of a system for performing the claimed technique (Pet. 9):

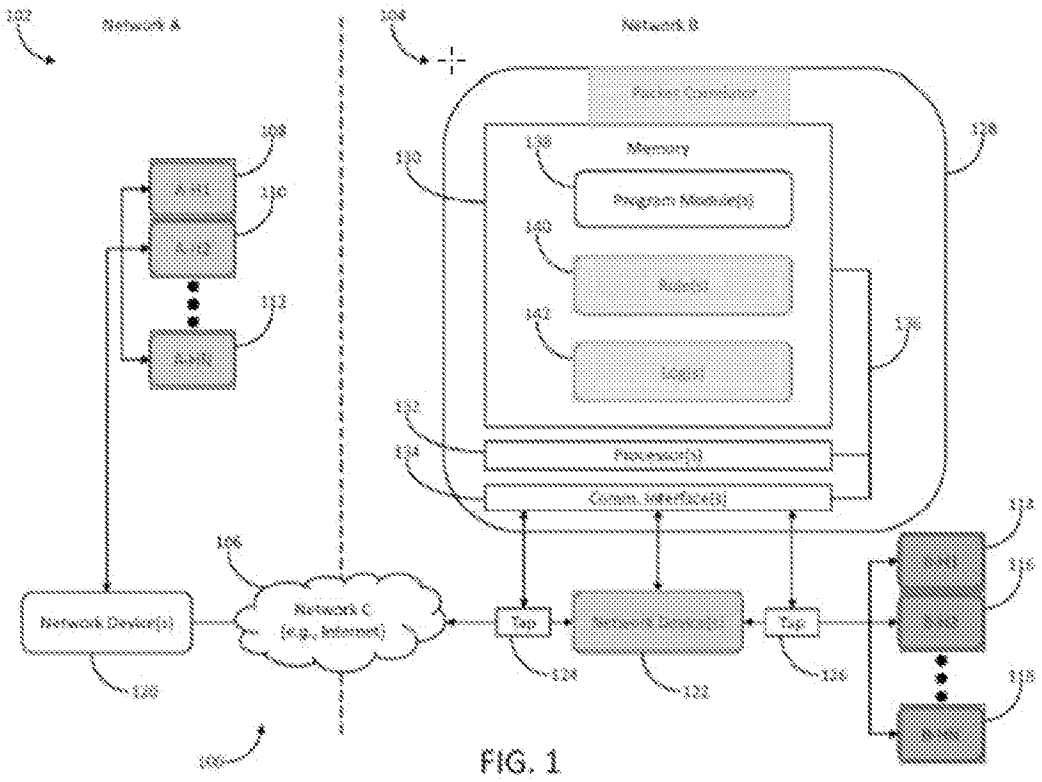

FIG. 1

Figure 1, reproduced above (as annotated by Petitioner), depicts an environment for correlating packets in communications networks. Ex. 1001, 2:7–9. The system includes network device 122, in green, that communicates with packet correlator 128. The packet correlator includes rules 140 and logs 142, shown in yellow. Taps 124 and 126 are located on either side of the network device and also communicate with the packet correlator. The components are arranged such that network traffic between, for example, host A-H1 in Network A, in blue, and host B-H1 in Network B, in red, would pass through a tap, then the network device, then the other tap.

The '903 patent explains that, in the case of packets moving from Network B to Network A, the network device "may include one or more

devices that alter one or more aspects of the packets . . . in a way that obfuscates the association of the packets received from" the Network B host and the corresponding packets generated by the network device and sent to the Network A host. *See* Ex. 1001, 5:8–21. For example, the network device "may be configured to perform network address translation (NAT) for network addresses associated with [Network B]," such that "the packets received from host [B–H1] . . . may comprise network- or transport-layer header information identifying their source as a network address associated with host [B–H1]," but the corresponding packets generated by the network device "may comprise network- or transport-layer header information identifying their source as a network address associated with [the network device]." *Id.* at 5:23–37.

The '903 patent's method is described in connection with Figures 2A–D. At step 1, the packet correlator generates rules that are supplied to the taps at steps 2 and 3. *See* Ex. 1001, 3:34–51. At step 4, host B-H1 transmits data (packets P1, P2, and P3) destined for host A-H1. *See id.* at 3:52–62. At steps 5 and 6, if the packets match the rules provided to tap 126, that tap sends log data to the packet correlator. *See id.* at 3:62–4:10. At step 7, the network device 122 receives packets P1, P2, and P3, modifies them, and sends the modified packets on towards host A-H1 as packets P1', P2', and P3'. *See id.* at 5:4–6:10. Those packets may, for example, have new address information. As the modified packets matching the rules pass though tap 124, that tap sends log data to the packet correlator. *See id.* at 6:10–34. Steps 10–15 repeat that process, where data is being sent from host B-H2 to host A-H1. *See id.* at 6:60–8:46.

At step 16, the packet correlator "may utilize log(s) 142 to correlate the packets transmitted by network device(s) 122 with the packets received by network device(s) 122." *Id.* at 8:47–49. This may be done by comparing "network-layer information, transport-layer information, application-layer information, or environmental variable(s)" and/or "timestamps" of the log entries. *See id.* at 8:49–9:44.

Steps 17 and 18 show data sent from host B-H2 to host A-H2 that does not match rules in the taps and that thus is not logged. *See id.* at 9:45–10:13. Steps 19–24 show data being sent from host B-H1 to host A-H1 that does match rules and is logged. *See id.* at 10:14–11:60.

Step 25 is another correlation, in which network-layer information, transport-layer information, application-layer information, environmental variables, and/or time stamps are used to correlate packet P10' with packet P10. *See id.* at 11:60–12:55. Then, in step 26, "[r]esponsive to correlating the packets," the packet correlator "may determine, based on one or more of the entries in log(s) 142, a network address associated with a host located in network [B] that is associated with a packet transmitted by network device(s) 122." *Id.* at 12:55–62. For example, "responsive to correlating P10' with P10," the packet correlator "may determine . . . that the network address associated with host [B-H1] is associated with P10' (e.g., a communication with host [A–H1])." *Id.* at 12:62–67.

At step 27, the packet correlator "may generate one or more messages identifying [host B–H1]." *Id.* at 12:66–13:1. "For example, host [A-H1] may be associated with a malicious entity," and the messages "may indicate that host [B-H1] communicated with host [A-H1] (e.g., the malicious

entity)." *Id.* at 13:2–7. The messages are sent to a user and an administrator at steps 28 and 29. *See id.* at 13:7–15.

At step 30, the packet correlator generates and updates the rules, for example, "to configure tap devices 124 and 126 to identify and drop packets received from host [B-H1]." *Id.* at 13:16–20. The packet correlator provisions the tap devices with the rules at steps 31 and 32. *See id.* at 13:20–23. Then, at step 33, host B-H1 communicates one or more packets but, at step 34, tap 126 identifies and drops the packets to prevent the spread of the malware. *See id.* at 13:23–28.

C. *Illustrative Claim*

Petitioner challenges claims 1–18, with claims 1 and 10 being independent. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

> 1. A method comprising:
>
> determining, by a computing system, that a network device has received, from a first host located in a first network, a plurality of first packets corresponding to first requests for content from a second host located in a second network, wherein the network device comprises a proxy;
>
> determining, by the computing system, that the network device has generated a plurality of second packets corresponding to second requests, wherein the second requests correspond to the first requests, and wherein the second requests are configured to cause the second host to transmit, to the network device, the content;
>
> generating, by the computing system, a first plurality of log entries corresponding to the plurality of first packets, wherein each of the first plurality of log entries comprises a receipt timestamp indicating a packet receipt time, and wherein the first plurality of log entries comprise first data from the first requests;
>
> generating, by the computing system, a second plurality of log entries corresponding to a plurality of second packets,

wherein each of the second plurality of log entries comprises a transmission timestamp indicating a packet transmission time, and wherein the second plurality of log entries comprise second data from the second requests;

determining, by the computing system and for each transmission timestamp, differences between at least one packet transmission time indicated by transmission timestamps and at least one packet receipt time indicated by receipt timestamps;

correlating, based on the differences and by comparing the first data and the second data, at least a portion of the plurality of first packets and at least a portion of the plurality of second packets; and

responsive to the correlating:

generating, by the computing system, an indication of the first host; and

transmitting, by the computing system, the indication of the first host.

Ex. 1001, 15:20–60.

D. *Asserted Ground of Unpatentability*

Petitioner asserts the following ground of unpatentability (Pet. 5):

Challenged Claims	Basis	References
1–18	§ 103[2]	Paxton[3], Sutton[4], and Ivershen[5]

Petitioner's challenges are supported by the Declaration of Dr. Robert Akl (Ex. 1003).

[2] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the '903 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

[3] U.S. Pat. Application Publication No. 2014/0280778 A1 (published Sept. 18, 2014) (Ex. 1004).

[4] U.S. Patent No. 8,413,238 B1 (issued Apr. 2, 2013) (Ex. 1007).

[5] U.S. Patent No. 8,219,675 B2 (issued July 10, 2012) (Ex. 1005).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). The resolution of this question is important because it allows us to "maintain[] objectivity in the obviousness inquiry." *Ryko Mfg. Co. v. Nu–Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). In assessing the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation omitted). Generally, it is easier to establish obviousness under a higher level of ordinary skill in the art. *Innovention Toys, LLC v. MGA Entm't, Inc.*, 637 F.3d 1314, 1323 (Fed. Cir. 2011) ("A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse.").

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention of the '903 patent "had a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and approximately 2–3 years of experience in the design or development of telecommunication systems, or the equivalent." Pet. 13 (citing Ex. 1003 ¶¶ 18–20). Petitioner further notes that "[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education." *Id.* Patent Owner's proposed

level of ordinary skill is similar, with Patent Owner contending that the ordinary skilled artisan "would be someone with a bachelor's degree in computer science, electrical engineering, or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field." PO Resp. 12 (citing Ex. 2019 ¶¶ 27–31). Similar to Petitioner, Patent Owner also states that a person of ordinary skill in the art "may have additional industry experience in lieu of a formal degree." *Id.* at 13.

In the Institution Decision, we adopted Petitioner's assessment of the level of skill in the art. Dec. 21. Patent Owner offers a different formulation in the Response, but neither party provides substantive argument as to why its proposed level of skill is correct. *See* Pet. 13; PO Resp. 12–13. We do not find a material difference between the parties' proposals.

Based on this record, we apply the level of skill laid out in our Institution Decision because it is consistent with the level of ordinary skill in the art at the time of the invention as reflected in the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Accordingly, we find for the purpose of this Decision and based on the record before us, that a person of ordinary skill in the art at the relevant time would have a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and approximately 2–3 years of experience in the design or development of telecommunication systems, or the equivalent. We note, however, that our determinations on patentability would not change if we accepted Patent Owner's proposed level of skill.

B. Claim Construction

In an *inter partes* review proceeding, a patent claim shall be construed 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). 37 C.F.R. § 42.100(b) (as amended Oct. 11, 2018). This rule adopts the same claim construction standard used by Article III federal courts, which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. Under this standard, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *See Phillips*, 415 F.3d at 1312–13.

We construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." 37 C.F.R. § 42.100(b) (2020). Under *Phillips*, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner asserts "no terms require construction." Pet. 13. Patent Owner discusses its views as to the plain and ordinary meaning of "responsive to the correlating . . . transmitting, by the computer system, the indication of the first host," "determining . . . differences between . . . packet

transmission time . . . and packet receipt time," "network-interface identifier," and "encapsulating." PO Resp. 13–25.

After review of the current record, we conclude that no express claim construction is necessary for the purposes of this Decision. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

C. Obviousness of Claims over Paxton, Sutton, and Ivershen

Petitioner asserts that claims 1–18 are unpatentable under 35 U.S.C. § 103(a) as obvious over Paxton, Sutton, and Ivershen, citing the Declaration of Dr. Robert Akl for support. Pet. 5. To support its contentions, Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 14–70. Patent Owner opposes Petitioner's contentions with the support of Michael Goodrich, Ph.D. *See* PO Resp., Ex. 2019.

1. Paxton (Ex. 1004)

Paxton is titled "Tracking Network Packets Across Translational Boundaries," and "relates generally to identifying network packets, and more particularly, to determining the identity of network packets as they traverse boundaries that perform Network Address Translation (NAT)." Ex. 1004, code (54), ¶ 2. Paxton's method for tracking network packets (i) calculates a first hash of a packet application layer payload at an inside sensor before a boundary located between a client and a server, (ii) stores a first hash data record at a device that has direct access to the inside sensor, (iii) calculates a second hash of the packet application layer payload at an

outside sensor after the boundary, (iv) stores a second hash data record at a device that has direct access to the outside sensor, (v) transmits the packet from the client to the server, or from the server to the client, and (vi) determines whether the first hash data record and the second hash data record match. *Id.* at code (57). The first hash data record and second hash data record may include a hash value, an IP address, and a timestamp. *Id.* Paxton explains that the ability to identify the true source of a packet transmission through a boundary can provide significant benefits to network security—e.g., by enabling identification of nodes that are infected with malicious content, and by enabling attribution of malicious activity sensed at the edge of a network back to its original source. *Id.* ¶ 30.

Figure 1 of Paxton is reproduced below.

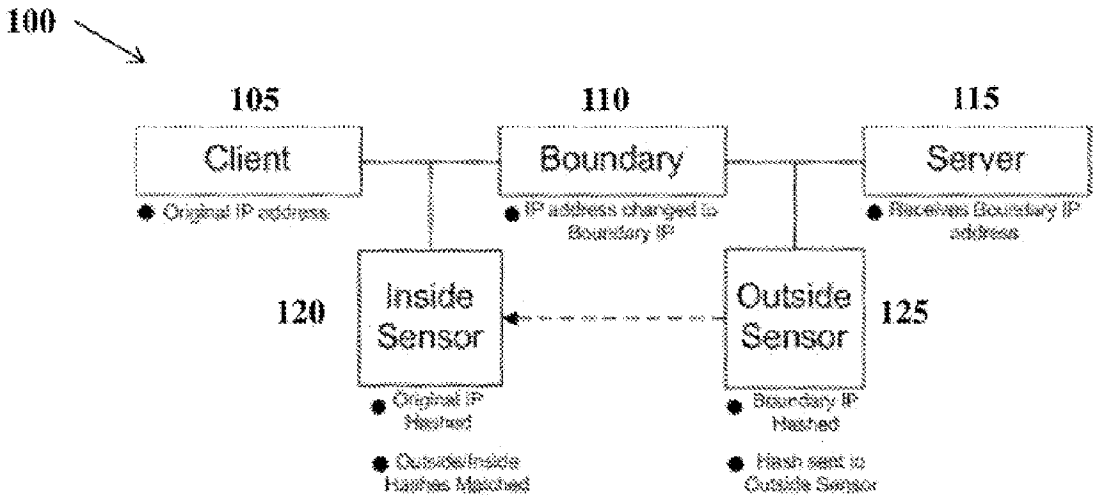

Figure 1, reproduced above, shows system diagram 100 for tracking packets across translation boundaries. *Id.* ¶¶ 11, 15. Packets are sent from client 105 across boundary 110 to server 115. *Id.* ¶ 16. When a packet is transmitted from client 105, inside sensor 120 calculates a hash, e.g., an MD5 algorithm hash, of the application layer payload, and stores it along with the network layer header. *Id.* ¶ 17. After the packet traverses boundary

110, outside sensor 125 calculates a hash of the payload along with the header data of the packet. *Id.* Inside sensor 120 and outside sensor 125 can be two commodity servers running full packet capture, with inside sensor 120 passively recording traffic on client 105 network before the contents are altered by the boundary, and outside sensor 125 passively recording traffic externally after it has been modified by the boundary. *Id.* ¶ 18. Paxton explains that payloads can be matched based on at least three criteria (hash, time, and IP address), such that when an identical hash is observed on outside sensor 125 and inside sensor 120, there is a high probability that the hashes belong to the same payload. *Id.* ¶ 21. Hashes from inside sensor 120 and outside sensor 125 can be matched via a first-in-first-out queue based on recorded timestamps in the first hash data record and second hash data record. *Id.* ¶ 22. For example, after a hash is observed on the outside, the closest matching hash (with respect to the timestamp) on the inside can be identified as the corresponding match, and the combination of identifiable inside and outside header data can serve as the identity of the packet. *Id.* Figure 3 of Paxton, reproduced below, is a diagram illustrating a first-in-first-out matching approach. *Id.* ¶¶ 13, 24.

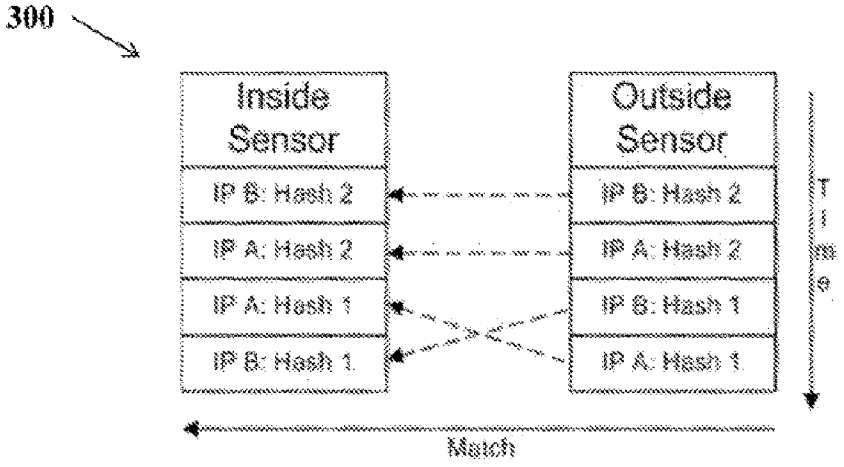

Figure 3, reproduced above, shows four packets that have been hashed by both inside sensor 120 and outside sensor 125, including two packets, 1 and 2, sent from both IP A and IP B (for a total of four packets). *Id.* ¶ 24. Figure 3 shows what happens when packets are sensed in a different order across boundaries. *Id.* In Figure 3, each of IP A and IP B sends two messages that are the same (IP A:Hash 1 and IP A:Hash 2 are equal, and IP B:Hash 1 and IP B:Hash 2 are equal). *Id.* The initial order of which the packets were sent from the original source was IP A:Hash 1, IP A:Hash 2, IP B:Hash 1, and IP B:Hash 2. *Id.* However, the order of which the packets were sensed by inside sensor 120 was IP B:Hash 2, IP A:Hash 2, IP A:Hash 1, and IP B:Hash 1, while the order of which the packets were sensed at outside sensor 125 was IP B:Hash 2, IP A:Hash 2, IP B:Hash 1, IP A:Hash 1. *Id.* Therefore, IP B:Hash 2 was the first message recorded in both inside sensor 120 and outside sensor 125, and even though this packet has the same hash value of IP B:Hash 1, since it was sensed first on both sides, the sensed packets can be matched together first. *Id.* ¶ 25. However, next packets IP A:Hash 1 and IP B:Hash 1 were sensed in a different order across inside sensor 120 and outside sensor 125. *Id.* ¶ 25. Since IP A:Hash 1 and IP B:Hash 1 have different hash values, the matching module does not consider them for matching; instead, the matching module finds the match at the next available matching hash, which was IP A:Hash 1. *Id.* The matching module can then conclude with the final match IP B:Hash 1. *Id.*

Paxton explains that the system for matching cryptographically hashed payloads as described so far, assumes that the payloads sensed both inside and outside are identical. *Id.* ¶ 28. According to Paxton, if either payload has been altered (e.g., by non-transparent proxies that can make

slight modifications to the payload to perform a media type transformation, protocol reduction, or anonymity filtering), the computed hash will not be the same, and therefore, will not match. *Id.* Paxton explains that

> different classes of hashing techniques could be leveraged in order to account for slight variations in payload alterations. For example, fuzzy hashing may be able to match payloads that have been slightly altered, as in the case of non-transparent proxies or deep packet inspection platforms. Fuzzy hashing is similar to traditional cryptographic hashing; with the exception that it produces a result value that is reflective of how similar the original data is to the altered data.
>
> *Id.* ¶ 29.

2. Sutton (Ex. 1007)

Sutton is titled "Monitoring Darknet Access to Identify Malicious Activity," and "relates to identification of potentially malicious activity based upon access attempts to darknet addresses." Ex. 1007, code (57), 2:7–10. Sutton discloses a technique of monitoring darknet access by: identifying a list of darknet addresses; monitoring communications originating from a protected network; comparing destination addresses of the monitored communications originating from the protected network to the list of darknet addresses; and, if a match is found between the destination addresses and the list of darknet addresses, providing notification of potential malicious activity originating from the protected network. *Id.* at 2:10–19.

Figure 2 of Sutton is reproduced below.

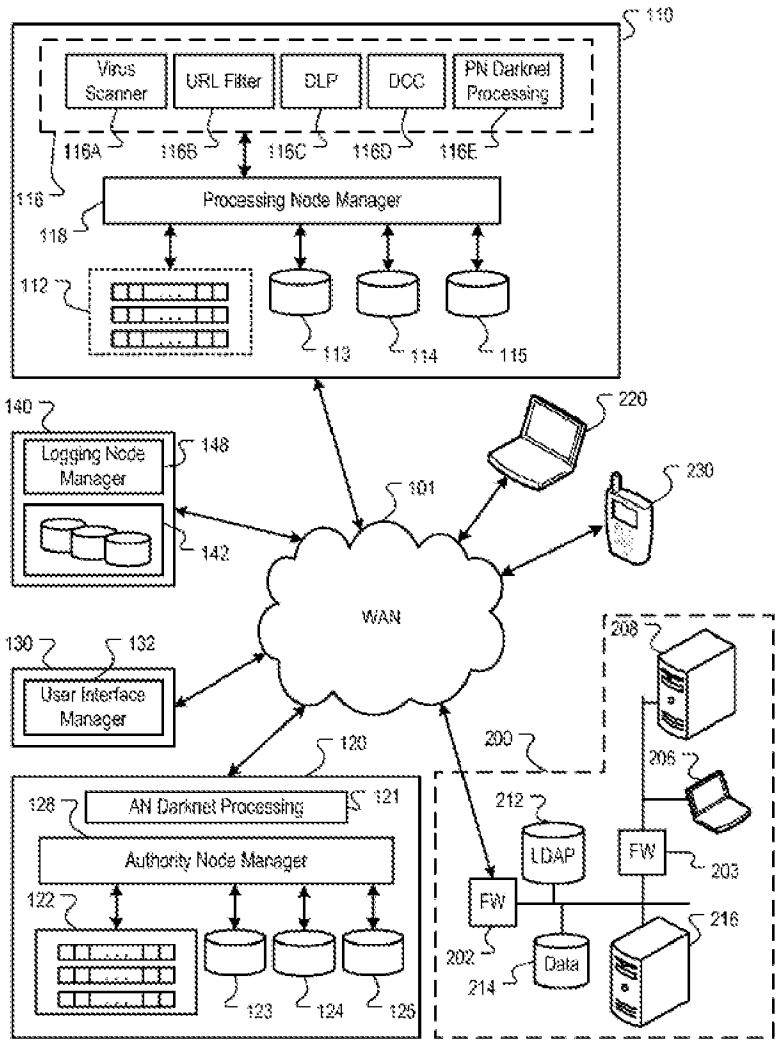

FIG. 2

Figure 2, reproduced above, is a block diagram of distributed security system 100. *Id.* at 2:29–31, 2:42–43. Distributed security system 100 includes: one or more component processing nodes 110; an authority node 120; logging node 140; external systems 200 (an enterprise), 220 (a computer device), and 230 (a mobile device); and wide area network (WAN) 101, such as the Internet, connecting the nodes and the external systems. *Id.* at 5:6–43. Each processing node 110 stores: security policies 113 received from authority node 120; detection process filter 112 and/or threat data 114

to facilitate a decision of whether a content item should be processed for threat detection; processing node manager 118 that can manage each content item in accordance with security policy data 113, detection process filter 112, and/or threat data 114; and data inspection engines 116. *Id.* at 5:45–6:17.

Each processing node 110 monitors content items requested by or sent from external systems 200, 220 and 230. *Id.* at 5:47–50. Each data inspection engine 116 can be configured to perform a threat detection process to classify content items according to a threat classification for a corresponding threat. *Id.* at 6:3–22. For example, the data inspection engines can include: a virus scanner engine 116A that can classify a content item as infected or clean; a network URL filter 1168 that can classify a URL address as allowed or restricted; a data leakage protection (DLP) engine 116C that can identify a content item as secure or leaking; a dynamic content categorization (DCC) engine 116D that can classify a content item as passed or failed; and a PN darknet processing 116E operable to identify darknet addresses. *Id.* PN darknet processing 116E identifies darknet addresses of darknets (that malicious code, such as code performing automated scanning, attempts to access) and store the darknet addresses in a darknet address database 115. *Id.* at 1:51–57, 6:14–22. PN darknet processing 116E can also interrogate communications to determine whether the communication is associated with (e.g., destined to, or originating from) an address in the darknet address database 115. *Id.* at 6:18–22.

Authority node (AN) 120 includes AN darknet processing 121 that identifies darknet address space and store a list of darknet addresses in

darknet address store 125. *Id.* at 7:28–35. AN darknet processing 121 also can distribute the list of darknet addresses to processing node(s) 110. *Id.*

Figure 4 of Sutton is reproduced below.

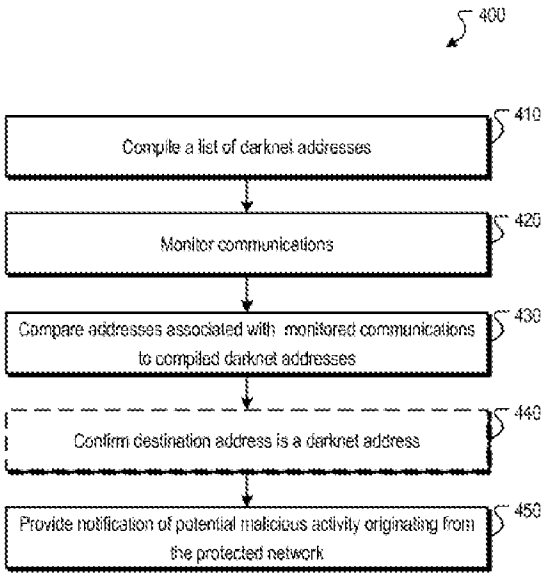

FIG. 4

Figure 4 of Sutton, reproduced above, illustrates a method for identifying malicious activity based upon darknet access. *Id.* at 2:24–25. A list of darknet addresses is compiled in step 410 by one or more authority nodes in conjunction with one or more processing nodes. *Id.* at 11:37–41. Once a list of darknet addresses is received from an authority node, processing node 110 can begin monitoring communications. *Id.* at 10:39–41. Processing node 110 inspects all or some communications for inclusion of a destination address that is included in the list of darknet addresses, and can identify communications that purport to originate from the darknet address space. *Id.* at 10:41–45. Communications are monitored in step 420 by one or more processing nodes. *Id.* at 12:25–35. The addresses associated with monitored communications in step 430 are compared to compiled darknet addresses, and if there is a match between destination addresses and

the list of darknet addresses, the communication can be inferred to be indicative of malicious activity. *Id.* at 12:36–45. Optionally in step 440, the identified destination address from step 430 can be confirmed to be a darknet address by, for example, using a scanner associated with the processing node to send a connection request to that identified the destination address. *Id.* at 12:45–56. If a device responds to the connection request then the address is removed from the list of darknet address, but if no device responds then the address is identified as malicious. *Id.*

Notification of potential malicious activity can be provided in step 450 by one or more processing nodes and/or by an authority node. *Id.* at 12:57–13:9. This notification can be provided to (i) an administrator of a protected enterprise network, (ii) a special purpose application operable to inspect a device for malicious program code and to remove malicious program code from the device, if found, or (iii) other processing nodes with instructions to provide filtering or detailed inspection of communications identified as similar (e.g., based upon an origination address). *Id.* The communication can be also flagged as potentially malicious. *Id.* Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules. *Id.*

3. Ivershen (Ex. 1005)

Ivershen is titled "System and Method for Correlating IP Flows Across Network Address Translation Firewalls." Ex. 1005, code (54). Ivershen relates to "correlating packets in a telecommunications network and, more specifically, to correlating packets with address information that has been modified by a Network Address Translation (NAT) firewall." *Id.* at 1:8–12. In Ivershen's method, data packets are captured from a first

interface using a monitor probe coupled to the first interface, and are correlated into a first group of session records, and for each of the first group of session records, a correlation key is created using data in one of the packets in the session record. *Id.* at code (57). Data packets also are captured from a second interface using a monitor probe coupled to the second interface, and are correlated into a second group of session records, and for each of the second group of session records, a correlation key is created using data in one of the packets in the session record. *Id.* The correlation key for one of the first group is compared to the correlation keys for each of the second group of session records to identify session records with matching correlation keys. *Id.*

i. *Claim 1*

As an initial matter, we must determine what allegations are properly before us in regards to the limitation which states "responsive to the correlating: generating, by the computing system, an indication of the first host; and transmitting, by the computing system, the indication of the first host" and the associated motivation to combine Paxton and Sutton.

Petitioner asserts that "Paxton discloses, responsive to the correlating (responsive to finding a match), generating, by the computing system, an indication of the first host (generating a match log including the identity of the packet source address)." Pet. 39. Petitioner goes on to state that "Paxton discloses correlating packets to identify malicious activity and leaves specific usage and remedial steps to a POSITA" and that "[a] POSITA would have been motivated to transmit the indication of the first host, e.g., to an administrator, as taught by Sutton, responsive to the correlating disclosed by Paxton." *Id.* at 40. In describing the motivation to combine Paxton and

Sutton, however, Petitioner makes the following statement

> ***To the extent Patent Owner argues that Paxton does not explain in detail what actions are taken with respect to identified malicious activity***, a POSITA would have been motivated to modify Paxton's computing system to, after the correlating, notify administrators of devices involved with the malicious activity (e.g., as in claim limitations [1g], [10h]) and generate rules to be provisioned to a packet-filtering device (e.g., a gateway, server, or packet inspecting device within the system such as, but not limited to, Paxton's sensor 120 and/or boundary 110, which are, e.g., servers, gateways, and firewalls in the first network; or, alternatively, a similar but separate device in Paxton's multi-device system performing inspecting and filtering functions that would have been included in the first network alongside Paxton's plural sensor and boundary devices to the extent Patent Owner argues a separate device is required) and used for identifying, filtering, and/or blocking host devices' future packet communications (e.g., as in claims 8-9, 17-18), as taught by Sutton.

Pet. 21 (emphasis added). Petitioner goes on to argue that "when a packet is detected as communicated to/from a darknet address (post-boundary), and Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary), ***Sutton teaches making that identification known to administrators*** and/or implementing rules to identify or drop future packets to prevent further malicious communications." *Id.* at 22 (emphasis added).

In the Institution Decision, the Majority preliminarily found that "Paxton suggests administrators should be informed of the true source discovered by correlating thus meeting the claim language—i.e., responsive to the correlating: . . . transmitting, by the computing system, the indication of the first host." Dec. 38–39. We further noted that "[b]ecause Paxton ties the identifying nodes to the finding of a 'true source' there is no need to combine with Sutton's method of determining when to notify

administrators." *Id.* at 39. Finally, we preliminarily concluded that "Petitioner does not need to rely on Sutton's determining that a device is potentially infected with malicious software code to trigger sending notifications because Paxton suggests sending a notification in the discussion of determining the 'true source' of a packet." *Id.* As to a motivation to combine Paxton and Sutton, we stated that "we rely on the explicit motivation in Paxton rather than the generic motivation provided in the Petition at pages 21–22." *Id.* at 40.

Patent Owner argues that we "impermissibly departed from the Petition and instituted IPR based on [our] own obviousness ground." PO Resp. 24 (citing *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1336 (Fed. Cir. 2020) ("[T]he Board does not enjoy[] a license to depart from the petition and institute a different inter partes review of his own design.") (internal quotation marks and citations omitted)). Patent Owner asserts that we improperly departed from the challenges in the Petition by relying on Paxton for the recited transmitting responsive to the correlating in place of Sutton, and thereby created a new motivation to combine. *Id.* at 24–25. Petitioner contends that the majority

> correctly recognized, [that] Paxton alone at least teaches or suggests the 'responsive to' limitation of claim 1. Therefore, the Majority did not need to reach whether it would have been obvious to modify Paxton's computing system in view of Sutton's teachings to render claim 1 obvious. The Majority did not 'impermissibly depart[] from the Petition,' as PO incorrectly argues because for claim 1 the Petition presented Paxton as modified by Sutton as an ***alternative*** to Paxton alone.

Reply 13 (internal citations omitted) (emphasis in original).

As the Supreme Court has stated, "in an inter partes review the petitioner is master of its complaint and normally entitled to judgment on all

of the claims it raises." *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018). Thus, the question before us is whether Petitioner raised a challenge in which it alleges that Paxton alone is sufficient to render obvious the recited transmitting responsive to the correlation. There is language in the Petition's motivation to combine section asserting that "to the extent" that Patent Owner argues that Paxton is insufficient then Sutton teaches the recited actions taken in response to malicious activity, including transmitting the identity to the administrators. *See* Pet. 21–22. That would seem to indicate that the inclusion of Sutton is an alternative theory.

The question that persists, however, is what is the other argument for which Sutton's teachings may stand in place. Petitioner provides a description of the disclosures of Paxton, but that description does not mention transmitting any notification to the administrator. *See* Pet. 14–16. In the motivation to combine section, Petitioner states that "Paxton leaves, to a POSITA, remedial steps (e.g., uses of the correlation results), which are taught by Sutton." *Id.* at 22; *see also id.* at 23 (arguing that modifying Paxton to include Sutton's teaching of "generating notification messages . . . would have been obvious and well within the skill of a POSITA."). In the claim chart, Petitioner cites Paxton's disclosure of identifying the true source of a packet as a benefit to network security, which "**can provide a way to quickly identify nodes that are infected with malicious content, which can allow the network administrator to better identify the scope of the malicious incident**." *Id.* at 40 (quoting Ex. 1004 ¶ 30) (emphasis in Petition). At Institution, we found that language to be persuasive evidence that Paxton teaches or at least suggests the recited transmitting. *See* Dec. 38–39. Upon reflection on the full record, however, this does not appear to

be Petitioner's argument. On that very same page of the claim chart, Petitioner argues that "[a] POSITA would have been motivated to transmit the indication of the first host, e.g., to an administrator, *as taught by Sutton*, responsive to the correlating disclosed by Paxton." Pet. 40 (emphasis added). Thus, it appears that we gave weight to the citation from Paxton that differs materially from the argument crafted by Petitioner. Therefore, the argument that must be evaluated is whether Paxton as modified by Sutton would have taught the recited transmitting responsive to the correlation.

As such, we turn to Petitioner's proffered argument for the "responsive to the correlating" limitations. Petitioner contends Paxton discloses "generating . . . an indication of the first host" and "identify[ing] the true source of packet transmission through a boundary." Pet. 39–40. Here, Petitioner relies on Paxton's disclosure "of a log that illustrates a matching payload . . . . In this case, the identity of the packet is the SrcAddr (source address) of the packet sensed from each side." *Id.* at 40 (emphasis omitted). Further, Petitioner contends that Paxton suggests that identifying the true source of a packet can help "identify nodes that are infected with malicious content . . . sensed at the edge of the network back to its original source." *Id.* As to the transmitting, Petitioner relies on Sutton's disclosure of "monitor[ing] communications to identify access attempts to/from darknet addresses" and that "[s]uch attempts can be inferred to be associated with malicious activity and a notification or other corrective action can be provided identifying such potentially malicious activity." *Id.* at 41 (citing Ex. 1007, code (57), 10:60–11:3–18) (emphasis omitted).

Therefore, the combination asserted by Petitioner is one in which "a packet is detected as communicated to/from a darknet address (post-

boundary)," "Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary)," and "Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications." *Id.* at 22. Petitioner contends that this combination would only involve "[t]he application of known techniques (e.g., Sutton's implementation of rules and data to define security policies, disallowed websites, etc.) to improve similar devices (e.g., servers, gateways, firewalls, etc. in Sutton's and Paxton's systems) to provide predictable results in the same way (e.g., to provide packet-filtering functions preventing communications with potentially malicious hosts)." *Id.* at 22–23.

Patent Owner argues that this combination is insufficient to teach the disputed limitation. PO Resp. 28–44. Patent Owner contends that Petitioner does not explain why any such transmitting would be responsive to the correlation as required by the claims. *Id.* at 30. In particular, Patent Owner asserts that the proposed combination "would simply result in notifying administrators of potentially infected devices in reaction to finding that 'a packet [has been] detected as communicated to/from a darknet address (post-boundary).'" *Id.* (quoting Pet. 22). According to Patent Owner, this is not enough because "[t]he detection of darknet activity involves no correlation whatsoever . . . it simply involves a comparison of the original addresses information of a packet to a list of darknet addresses." *Id.* Patent Owner further argues that the recited responsiveness also is not taught by Paxton, which identifies a source of packet transmission without teaching any actions that occur responsive to that identification. *Id.* at 31. This assertion is supported by Patent Owner's Declarant, Dr. Goodrich, who opines that

"*Paxton* does not disclose or suggest doing ***anything*** with the packet matching information unless and until malicious activity is sensed. Although I note that Petitioner argues that *Paxton* 'generat[es] a match log including the identity of the packet source address,' *Paxton* does not disclose doing anything responsive to, or in reaction to, generating this match log." Ex. 2019 ¶ 83 (citing Pet. 39; Ex. 1004 ¶ 22).

Petitioner responds by arguing that Patent Owner's "assertion that Paxton does not disclose 'doing anything responsive to correlating packets,' is facetious: there would be no purpose in doing that determining at all if it was not recorded or otherwise made known." Reply 5. Petitioner further contends that "Paxton expressly teaches creating a log and notifying a network administrator of the identified host." *Id.* (citing Ex. 1004 ¶ 30, Fig. 2; Ex. 1003 ¶¶ 63, 119; Pet., 14–15, 40; Dec. 38–39). We, however, are not persuaded that this argument was articulated sufficiently in the Petition. Petitioner cites pages 14–15 of the Petition. That portion of the Petition states "[m]atching packets and identifying the true source of packet transmissions is useful for network security, providing a way to trace malicious activity sensed at the edge of a network and identify nodes infected with malicious content." Pet. 14–15. It is true that Paxton states that the ability to identify the true source of a packet transmission "can provide a way to quickly identify nodes that are infected with malicious content, which can allow the network administrator to better identify the scope of malicious content." Ex. 1004 ¶ 30. We find no argument in the Petition that asserts "allow[ing] the network administrator to better identify the scope of malicious content" means that a transmission is made (or any other action is taken) responsive to the correlation.

Sutton also fails to fill in this gap. Petitioner argues that "Sutton discloses transmitting the indication of the first host (e.g., notifying an administrator) responsive to identifying a device associated with malicious activity." Pet. 41. Sutton "monitors communications to identify access attempts to/from darknet addresses" and if such an attempt is found "a notification or other corrective action can be provided identifying such potentially malicious activity." *Id.* (quoting Ex. 1007, code (57)). Sutton further states that if devices associated with malicious activity "reside within the enterprise network, a notification 355 can be provided to the enterprise network (e.g., a network administrator) indicating that such devices are potentially infected with malicious software code." *Id.* (quoting Ex. 1007, 10:60–11:3). Sutton identifies malicious nodes by determining whether a communication is destined or originating from an address in the darknet address database. Ex. 1007, 6:15–22. Thus, if a darknet address is found then Sutton will transmit a message indicating the malicious presence. This leaves us with a correlation from Paxton with no specific actions taken post-correlation, and a transmission from Sutton unrelated to any correlation, but without the necessary bridge showing that one of ordinary skill in the art would have appreciated that the transmission would be responsive to the correlation. As such, Petitioner has not provided us with argument and evidence sufficient to establish by a preponderance of the evidence that claim 1 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

ii. *Claim 10*

Independent claim 10 is an apparatus claim that recites similar limitations to claim 1. Petitioner asserts that the combination of Paxton,

Sutton, and Ivershen teaches the limitations of independent claim 10. Pet. 58–63. We have reviewed the record and find that Petitioner's arguments and evidence are insufficient for substantially similar reasons as articulated above in regards to claim 1. As such, Petitioner has not demonstrated by a preponderance of the evidence that claim 10 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

iii. *Dependent Claims 2–9 and 11–18*

Petitioner asserts that the combination of Paxton, Sutton, and Ivershen teaches the limitations of dependent claims 2–9 and 11–18. Pet. 43–58, 63–70. Dependent claims 2–9 depend from claim 1 and dependent claims 11–18 depend from claim 10. Petitioner's arguments and evidence regarding the additional limitations of these dependent claims do not remedy the above discussed deficiency with the independent claims. As such, Petitioner has not demonstrated by a preponderance of the evidence that claims 2–9 and 11–18 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

III. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties' respective arguments, Petitioner has not shown by a preponderance of the evidence that each of claims 1–18 of the '903 patent are unpatentable.

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–18	§ 103	Paxton, Sutton, Ivershen		1–18
Overall Outcome				

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner has not shown by a preponderance of the evidence that claims 1–18 are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Scott McKeown
Mark D. Rowland
James R. Batchelder
Andrew Radsch
Victor Cheung
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
james.batchelder@ropesgray.com
Andrew.radsch@ropesgray.com
Victor.cheung@ropesgray.com

PATENT OWNER:

James Hannah
Jeffrey Price
KRAMER LEVIN NAFTALIS & FRANKEL
jhannah@kramerlevin.com
jprice@kramerlevin.com

Bradley Wright
Scott Kelly
Blair Silver
BANNER & WITCOFF, LTD
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
bsliver@bannerwitcoff.com