

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner

v.

WEBROOT INC.
Patent Owner

Case No. IPR2023-01050
Patent No. 8,763,123

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,763,123**

TABLE OF CONTENTS

I. INTRODUCTION	1
II. SUMMARY OF THE '123 PATENT.....	1
A. DESCRIPTION OF THE '123 PATENT	1
B. SUMMARY OF THE PROSECUTION HISTORY	7
C. SUMMARY OF THE EPO COUNTERPART APPLICATION	11
D. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	13
E. LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE ART	14
III. REQUIREMENTS UNDER 37 C.F.R. § 42.104	15
A. GROUNDS FOR STANDING UNDER 37 C.F.R. § 42.104(A)	15
B. IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	15
IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	15
A. GROUND 1: <i>ACKROYD</i> RENDERS CLAIMS 1, 3-4, AND 6-16 OBVIOUS.....	15
B. GROUND 2: <i>ACKROYD</i> IN VIEW OF <i>DAHLSTROM</i> RENDERS CLAIMS 2 AND 5 OBVIOUS	41
V. DISCRETIONARY DENIAL IS NOT WARRANTED	48
A. THE <i>ADVANCED BIONICS</i> FRAMEWORK FAVORS INSTITUTION UNDER § 325(D) 48	
B. THE <i>FINTIV</i> FACTORS FAVOR INSTITUTION	51
VI. CONCLUSION	57
VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	58
A. REAL PARTIES-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	58
B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2).....	58
C. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3)	58

I. INTRODUCTION

The claims of U.S. Patent No. 8,763,123 (“’123 Patent”) erroneously issued over the prior art during prosecution. Due to a possible clerical mistake or other issue, a claim limitation that the Examiner expressly relied upon to allow the claims to issue is not part of the record and is not included in the issued claims. Review is necessary at a minimum to account for this error. Further, prior art that was used to finally reject all claims in a European Counterpart application—U.S. Patent No. 7,269,851 (“Ackroyd”)—was submitted to the United States Patent and Trademark Office too late in the process to allow for full and fair consideration before the ’123 Patent issued. Because the as-issued claims of the ’123 Patent should be evaluated in view of this prior art, and because that analysis will lead to the conclusion that Claims 1-16 of the ’123 Patent are unpatentable as obvious, CrowdStrike, Inc. (“Petitioner”) respectfully requests *inter partes* review.

II. SUMMARY OF THE ’123 PATENT

A. Description of the ’123 Patent

The ’123 Patent describes a system and process for identifying vulnerabilities to malware on remote computers by receiving and using information about the security products operating on those remote computers. ’123 Patent (Ex. 1001), Abstract. Namely, “the present invention relates to a method and apparatus for determining the protection that a remote computer has from malware.” *Id.*, 1:12-14. In the context of the ’123 Patent, malware is understood to include malicious code

or objects, such as viruses, trojans, worms, spyware, adware, etc. *Id.*, 1:19-22, 8:1-4.

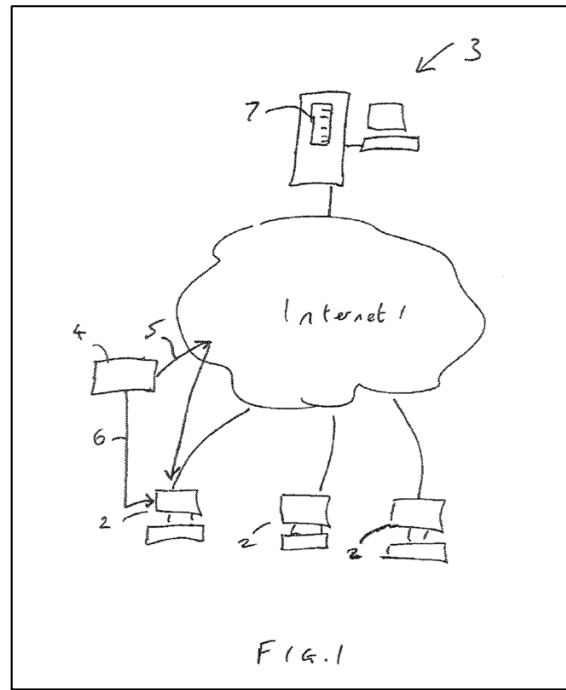
As described in the '123 Patent, traditional anti-malware products typically scan objects to look for signatures that are known to be indicative of malware. *Id.*, 1:23-34. Although this works for known malicious objects, there is, according to the '123 Patent, usually a delay between a new malware object being released and the development of known signatures for identifying that malware. *Id.*, 1:35-47. Known methods and systems suffer from this delay in between the time when the malware is released, and when the existing anti-malware techniques discover and distribute a signature for identifying the malware. *Id.*, 2:63-3:3. The '123 Patent characterizes these prior art methods and systems as “rel[ying] solely on signature matching[.]” *Id.*, 3:14-15.

In purported contrast to these known systems and methods, the '123 Patent allegedly describes techniques for “rapid determination” that overcome the need for detailed analysis of the object itself to determine whether or not the object is malware. *Id.*, 3:14-24. According to the '123 Patent, this can be accomplished by sharing data between several remote computers and a base computer. *Id.*, 3:25-36. That shared data about a potential malware object can include: “executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the

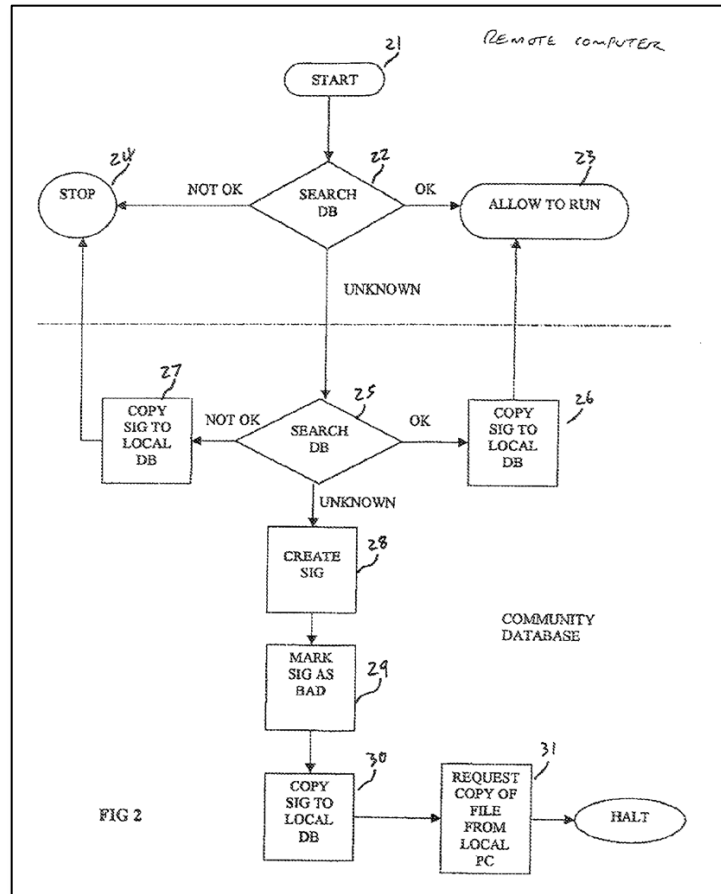
original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.” *Id.* In some embodiments, “the data is sent in the form of [a] key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers.” *Id.*, 3:48-56.

For example, several techniques are described to make a malware determination. One example involves “the concept of ancestry[.]” *Id.*, 6:13-19. In this way, as described in the ’123 Patent, “[t]he key relating to the first object may be inspected to identify a component that uniquely identifies the first object and that is inherited or otherwise present in the key of a descendant or other related object of the first object.” *Id.* In that instance, the method described will “automatically classify[] as malware any computer object that has a key in which said unique identifier component is present[,]” where the unique identifier is also associated with malware. *Id.*, 6:20-26. In other embodiments, the ’123 Patent describes “trusted installers,” and a method in which “any objects relating to or created by the trusted installer are automatically authorized to proceed.” *Id.*, 7:11-25.

The '123 Patent includes basic figures that purport to depict embodiments of the alleged invention. For instance, Figure 1 illustrates the apparatus in which various embodiments may be implemented:



Id., Fig. 1. Other figures illustrate flowcharts with the methods described and claimed in the '123 Patent:



Id., Fig. 2; *see also id.*, Fig. 3 (illustrating flow chart for creating and utilizing a mask); Fig. 4 (illustrating an information obtaining stage).

Stepping through the flowchart of Figure 2, the '123 Patent describes several processes for determining whether an object is safe, unsafe, or suspicious. *See generally id.*, 8:21-15:35. These five processes are characterized as “preferred central heuristics[.]” *See id.* First, the process uses “the singularity or plurality of names, locations, vendor, product, and version information captured and correlated from all of the remote computers 2 that have seen the object.” *Id.*, 10:43-46. Second, the process uses “an object’s relationship to other objects that act upon it or upon

which it acts.” *Id.*, 11:5-6. Third, the process involves time and volumes, and “[r]elevant data includes when the object was first seen, when it was last seen, how many times it 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.*, 11:60-64. Fourth, the process “considers the behaviour of an object[,]” which “allows a score to be developed based on the types of events performed by an object or events performed on it by itself or other objects.” *Id.*, 12:16-19. And finally, fifth, the process “considers the behavior of a web page or script.” *Id.*, 12:45-46. In all, the database in the system collects metadata from the remote computers, and that metadata can be used to define behavior across the community, or network. *Id.*, 13:54-65.

This metadata can also be used to identify vulnerabilities on particular remote computers. For instance, aspects of the present invention describe “a method of determining the protection that a remote computer has from malware,” comprising:

receiving at a base computer details of all or selected security products operating at a point in time on said remote computer; receiving similar information from other remote computers connected to the base computer; and, identifying any malware processes that were not identified by said other remote computers having that particular combination of security products.

Id., 5:25-36. Here, “the base computer can be used to obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a point in

time, renders a particular computer having those products and settings susceptible or vulnerable to any particular malware object.” *Id.*, 5:37-43. In other words, if a base computer knows that a computer has a certain version of an anti-virus product, and it knows that a malware process was not detected at that computer, then this information can be used to determine that the computer has a vulnerability to that malware process. *Id.*, 16:5-17:15. The user in that instance might be advised of the vulnerability, such as through a prompt to update anti-virus software. *See id.*, 16:5-17:15.

B. Summary of the Prosecution History

The application that issued as the '123 Patent was filed on July 8, 2012, as a divisional claiming priority to U.S. Patent Application No. 11/477,807, which was filed on June 30, 2006. '123 *File History* (Ex. 1002). The application also claimed foreign priority dating back to June 30, 2005. *Id.* Petitioner applies June 30, 2005, as the priority date for the Challenged Claims for the purposes of this proceeding only.

On April 15, 2013, an Office Action was transmitted and entered into the record that rejected all pending claims 1-9. *See id.*, 91-99 (Office Action dated April 15, 2013). Most of the claims, including independent claims 1 and 4, were rejected as obvious in view of prior art references Dahlstrom and Beddoe. *Id.* Dependent claims 3, 6, and 9, were rejected as obvious over Dahlstrom and Beddoe in further

view of Mateev. *Id.* In response, Applicant submitted claim amendments, and emphasized that “the claimed invention generally relates to a computer that provides information to a community database that is representative of all or selected ones of the software products loaded on or available [to] the computer.” *See id.*, 123-134 (Amendment dated July 15, 2013). The Applicant attempted to distinguish the Dahlstrom reference by stressing the ability to determine a computer’s vulnerability to malware based on the security products on that computer, asserting that “Dahlstrom fails to teach, disclose, or render obvious at least identifying one or more of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer; and identifying one or more malware processes that were not identified by the combination of security products operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.” *Id.*, 131-132.

Thereafter, another Office Action was transmitted on August 6, 2013, and in it the Examiner maintained the obviousness rejections based on Dahlstrom, Beddoe, and Mateev. *See id.*, 138-148 (Office Action dated August 6, 2013). In response, the Applicant requested and received an Examiner Interview. *See id.*, 160 (Interview Summary). The Applicant characterized the discussion and the “inventive concept” of the claimed invention, stating: “the inventive concept ‘Security products updated

on remote computers by central computer, and scanning for malware not detected on remote computers due to lack of updated antivirus software. Further Detection of malware on cloud of computer networks and updating of security products on computers.” *Id.* The Applicant then submitted a Request for Continued Examination on December 5, 2013. *See id.*, 164-180 (RCE Request).

After the Examiner Interview and after the Request for Continued Examination, the Applicant submitted a supplemental Information Disclosure Statement on December 12, 2013. *See id.*, 189-191. In that disclosure, the Applicant identified for the first time, *inter alia*, the Ackroyd reference (at the time, a pending application with Application No. 2003/0131256). Just over a month later, the Applicant’s representative and the Examiner conducted another Interview on January 14, 2014. *See id.*, 206 (Interview Summary). The purportedly allowable subject matter discussed in that interview involved “security products on multiple computers scanning remote computers, detecti[ng] malware in cloud by remote and base computers[.]” *Id.* As set out in the interview summary, this subject matter was recited in dependent Claim 3, and the Applicant’s representative and the Examiner discussed amending the claims to include this concept into the independent claims. *See id.* Nevertheless, promptly thereafter, a Notice of Allowability was entered into the record on January 29, 2014. *See id.*, 207-213 (Notice of Allowance). The Examiner did not require the limitations from Claim 3 to be included into the

independent claims. *See id.* Instead, the Examiner included an Examiner's Amendment with the Notice of Allowability, and that amendment required: "receiving, at a base computer, details uniquely identifying one or more security products...." *See id.*, 209 (emphasis in original denoting the Examiner's Amendment).

Importantly, the Examiner's Reasons for Allowance reference a "submission of amended claims on 1/21/2014[,]" but those amended claims do not appear in the record. *See id.*, 207; *see also generally id.*, 207-213 (Notice of Allowance). According to the Examiner's Reasons for Allowance, the allowable subject matter hinged on the following concept that was purportedly included in the missing claim amendments: "Detecting malware on remote computers by base computer, by comparing the security product(s) on remote and base computers, and comparing malware objects by size, name, logical storage and path of the malware object and details as described in the independent claim(s)." *See id.*, 212. One significant problem with the '123 Patent is that assuming it is true that the Applicant submitted amendments on January 21, 2014, and assuming those amendments included the allowable subject matter that the Examiner relied on in the Notice of Allowability, **those amendments are not included in the issued claims.** *See id.*, 207.¹ There is a

¹ All emphasis added unless noted otherwise.

disconnect in the record between what the Examiner seemed to think was allowable as compared to the claims that were ultimately issued. *See generally id.* The Applicant's representative noted this discrepancy in a letter to the Office dated April 29, 2014, but **the problem was never cured** and, instead, the Applicant's representative simply suggested that the entirety of the independent claims should be understood as allowable subject matter. *See id.*, 235-237 (Letter dated April 29, 2014).

C. Summary of the EPO Counterpart Application

On May 13, 2013, the Applicant of the '123 Patent in the United States filed a divisional application requesting a grant of a European Patent. *See EPO File History* (Ex. 1003). The application claims priority to GB Application No. 0513375.6 dated June 30, 2005, which is the same priority document listed on the face of the '123 Patent. *See id.*, 234-235 (Request dated May 13, 2013). On August 30, 2013, a European Search Report was entered, which identified a single document considered to be relevant—US Patent Application No. 2003/131256 to Ackroyd. *See id.*, 166-171 (European Search Report). In the corresponding opinion, the representative from the European Patent Office noted that Ackroyd was “very relevant for the present invention,” and noted that the reference disclosed the same concepts claimed. *See id.*, 169 (European Search Opinion). After several intervening changes to the applicant's representative on file and the applicant itself, examination

started on April 19, 2018. *See id.*, 121-125 (Communication dated April 26, 2018).

The examining unit rejected all the claims based on Ackroyd, noting that Ackroyd discloses the features of the claims. The correspondence did note that one feature seemed to be missing from Ackroyd—receiving at the base computer “details of processes run by said other remote computers that were not locally identified as being malware.” *See id.*, 124 (Communication dated April 26, 2018) That concept was ultimately deemed not patentable in the European Patent Office. Importantly, that limitation is not present in any of the Challenged Claims of the ’123 Patent.

After several sets of claim amendments and an oral hearing, the examining division issued a decision refusing the application. *See id.*, 47 (Decision dated July 25, 2019). In that decision, the division concluded that the claims were not inventive over Ackroyd. *See id.*, 54. The examining division found two alleged differences between the teachings of Ackroyd and the claims presented to the European Patent Office, namely that information about susceptibility to attack is provided to the user, and the database search is performed in a different way. *See id.*² But neither of these were sufficient to show an inventive step and merit a patent award. *See id.* Neither of these differences that the European Patent Office noted in comparing the claims

² The Applicant in the EPO has filed a notice of appeal, and the process is still pending. *See id.*, 33 (Notice of Appeal dated October 4, 2019).

to Ackroyd are present in any of the independent claims of the '123 Patent. *Compare id.*, 79-81 (Amended Claims dated May 31, 2019) (expressly including: (1) “providing information to the user...”; and (2) “searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected”) *with* '123 Patent at Claims. The first noted difference—involving providing information to the user—does appear in dependent claims 2 and 5 of the '123 Patent. But as described below, the prior art of record and expert analysis renders these claims unpatentable as obvious. The second noted difference—involving the database search—does not appear in any of the Challenged Claims. At bottom, the analysis and conclusion from the European Patent Office that the claims submitted there are not patentable in view of Ackroyd is **directly relevant** to the Challenged Claims and their patentability here.

D. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*).

In parallel litigation, PO argues all claim terms should be given their plain and ordinary meanings. Ex. 1008 (Dkt. 304, *Responsive Markman Brief*), 36-40. For the purposes of this proceeding only, Petitioner proposes the Board adopt PO's proposal.

See Western Digital Corporation v. Spex Technologies, Inc., IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018) (finding Petition based on claim constructions urged by Patent Owner satisfies the claim construction requirements and Petitioner is not required to express its subjective agreement regarding correctness of the proffered claim construction or take ownership of the construction); *see also General Electric v. Vestas*, IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018).³

E. Level of Skill of a Person Having Ordinary Skill in the Art

As of June 30, 2005, a person having ordinary skill in the art (PHOSITA) would be a person having a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of host monitoring systems, software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Dr. Jakobsson Declaration ("*Decl.*") (Ex. 1004), ¶¶54-56.

³ Petitioner reserves the right in other proceedings to construe the Challenged Claims and to argue they are indefinite.

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the '123 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

Petitioner requests the Challenged Claims be found unpatentable on the following grounds:

Proposed Ground of Unpatentability	Exhibits
Ground 1: Claims 1, 3-4, and 6-16 are obvious under § 103(a) over U.S. Patent No. 7,269,851 to Ackroyd (“ <i>Ackroyd</i> ”)	Ex. 1005
Ground 2: Claims 2 and 5 are obvious under § 103(a) over Ackroyd in view of U.S. Patent Publication No. 2004/0006704 to Dahlstrom et al. (“ <i>Dahlstrom</i> ”)	Ex. 1005 Ex. 1006

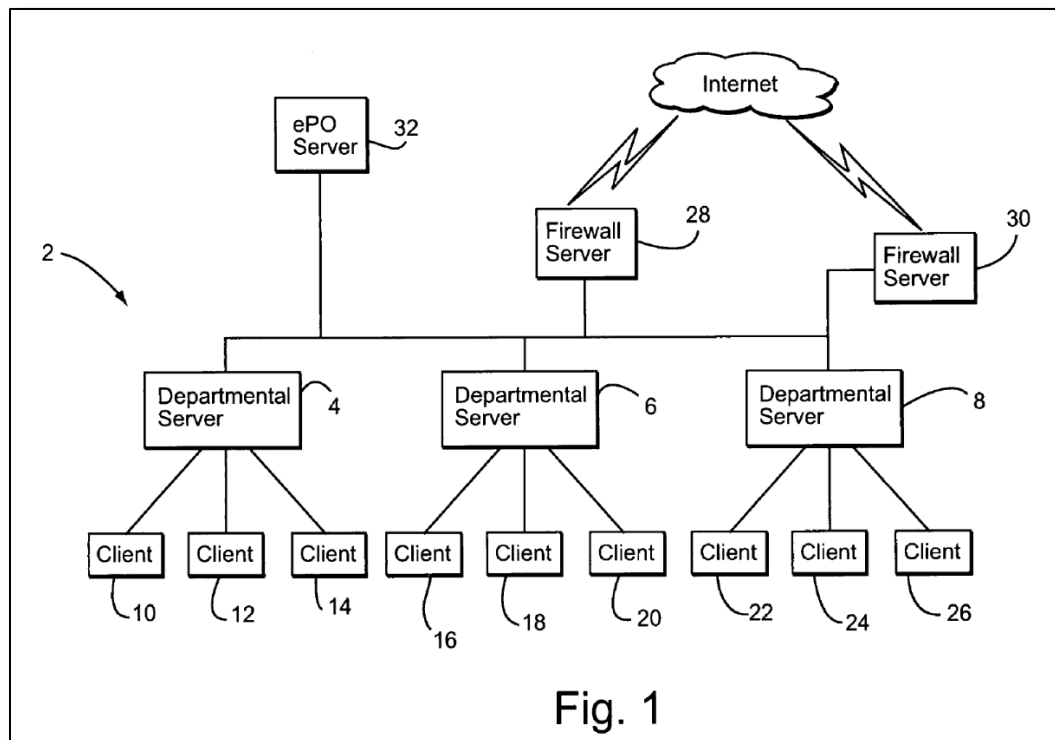
IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: *Ackroyd* Renders Claims 1, 3-4, and 6-16 Obvious

Overview of Ackroyd

Ackroyd was filed on January 7, 2002, published on July 10, 2003, and issued on September 11, 2007. *Ackroyd* therefore qualifies as prior art to the '123 Patent under 35 U.S.C. § 102(a), (b), and (e). In general, *Ackroyd* teaches “[a] managing computer within a computer network [that] serves to log messages received from individual computers within that computer network indicating detection of malware.” *Ackroyd*, Abstract. “The managing computer detects patterns of malware

detection across the network as a whole a[nd] triggers associated predetermined anti-malware actions.” *Id.* These actions “may include forcing specific computers to update their malware definition data, forcing particular computers to change their security settings and isolating individual portions of the computer network.” *Id.* An exemplary computer network is shown below:



Id., Figure 1. In various embodiments, the managing computer, also called the policy organising server,⁴ stores information received from remote computers in a database.

⁴ The inventor of Ackroyd, Mr. Robert John Ackroyd, lists a home address in Great Britain. Likely because of this, a few terms in Ackroyd use the British spelling, rather

Id., 2:56-61. “Such an arrangement allows convenient querying of the database, such as automatic running of predetermined queries, in order to detect particular patterns within the logged data messages and trigger appropriate responses.” *Id.* The database can include many types of information related to the security products used by remote computers in the network, including “the malware scanner products being used, the versions of the scanner engines and malware definition data being used, the security settings in force on the computer and the like.” *Id.*, 2:62-67. As noted in *Ackroyd*, “[t]his data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.” *Id.*, 2:67-3:4.

Ackroyd is analogous art to the ’123 Patent. First, *Ackroyd* is in the same field of endeavor as the ’123 Patent. For instance, the ’123 Patent states that “[t]he present invention relates generally to methods and apparatus for dealing with malware.”

than the American spelling. Most notably “organising” and “recognizing.” Rather than confusing the record with “[sic]” or bracketed changes each time these words appear, Petitioner has instead adopted the convention used in *Ackroyd* itself, and will also use the British spelling of these words where they come from that document.

'123 Patent, 1:9-10. Further, in the *'123 Patent*, “[t]he term ‘malware’ is used herein to refer generally to any executable computer file or, more generally ‘object,’ that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.” *Id.*, 1:19-22. Likewise, *Ackroyd* is in the same field of endeavor, and describes its field of invention as follows: “this invention relates to the field of malware protection, such as, for example, protection against computer viruses, worms, Trojans, banned files, banned words, banned images etc., upon a network of connected computers.” *Ackroyd*, 1:6-12; *Decl.*, ¶¶59-63 (additionally noting *Ackroyd* was used in EPO rejections as analogous prior art to the EPO counterpart application).

Second, *Ackroyd* is reasonably pertinent to a problem identified and purportedly solved by the *'123 Patent*. The *'123 Patent* describes a problem with existing malware detection as being slow to respond to new forms of malware, particularly in a network of remote computers. *'123 Patent*, 1:23-47 (describing existing malware products); 3:14-24 (describing the claimed invention as different from the prior art, and noting that the methods in the *'123 Patent* allow “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. Sophisticated pattern analysis can be carried out. This allows a rapid determination of the nature of the object to be made....”). Likewise, *Ackroyd*

teaches a solution to the same problem. *Ackroyd*, 1:21-37 (“As computer networks have become more widespread and complex, and the threats posed by newly developed types of malware more sophisticated and potentially damaging, it is important that malware protection is systematically and thoroughly implemented on a computer network. ... Given the threat posed by malware, such as the well known damaging effects of mass-mailing computer viruses, measures that can improve the effectiveness with which such threats can be dealt with are strongly advantageous.”); *Decl.*, ¶¶59-63. Because *Ackroyd* is in the same field of endeavor as the ’123 Patent, and additionally and separately because *Ackroyd* is reasonably pertinent to a problem the ’123 Patent purports to solve, *Ackroyd* is analogous art to the ’123 Patent.

1. Claim 1

1[Pre]. A method comprising:

Ackroyd describes systems and methods for managing malware protection in a computer network. *Ackroyd*, Abstract, 1:7-12, 1:41-58, claim 14 (“**A method** of managing malware protection...”); *infra*, Claims 1[a]-1[e].

[1(a)] receiving⁵, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;

Ackroyd discloses receiving information at a base computer, which is

⁵ PO has argued in the district court that the plain meaning of limitations 1(a)-1(e) (and the corresponding limitations in claims 4, 13, and 16) does not require the claimed steps to be

referenced as a malware policy organising server. That information includes details uniquely identifying one or more security products operating at a point in time on a remote computer.

For example, *Ackroyd* discloses a “malware policy organising server 32” (i.e., *base computer*) connected in computer network 2 which “serves to monitor and enforce security settings on all of the computers within the computer network 2.” *Ackroyd*, 3:40-44; *Decl.* ¶¶69-72 (noting the ’123 Patent, 7:64-8:1 describes that remote computers can be any device for loading and operating computer objects, including a server, such that a PHOSITA would have understood the plain meaning of “base computer” to similarly include a server). “The policy organising server 32 [] serves to receive logged data messages from the various different servers and client computers within the computer network 2 indicating detection of malware items by the malware scanners operating at those individual computers.” *Ackroyd*, 3:44-49.

Notably, the policy organising server 32 “also receives status information from the various computers indicating the malware scanning products being used, the scanner engine versions and virus definition data versions being used and

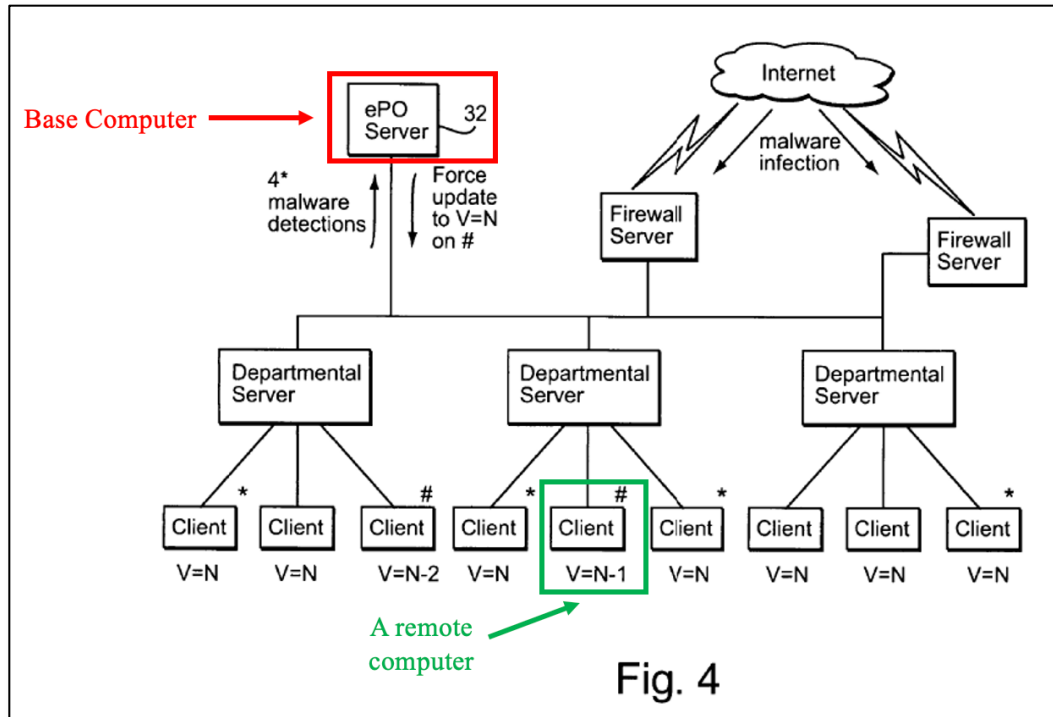
performed in any specific order. Ex. 1008 (Dkt. 304, *Responsive Markman Brief*), 46-48.

Petitioner asks the Board apply PO’s interpretation.

the security settings being applied within those different computers on the network” (i.e., *details uniquely identifying one or more security products*). *Id.*, 3:40-54 (emphasis added); *see also id.*, 2:62-3:4, 3:64-4:23; 4:43-5:39; *Decl.* ¶¶73-75 (noting this status information indicates the malware scanning products being used at the point in time the information was transmitted).

This data “uniquely identifies” one or more security products. For example, as claimed in claim 3, example details which uniquely identify a security product include “the name of the security products, versions, and loaded signature files.” ’123 Patent, claim 3. Consistent with this disclosure, as explained above, *Ackroyd’s* policy organising server 32 receives name and version details of the malware scanning products being used at the point in time the data was transmitted. *Id.*, 3:40-54 (emphasis added); *see also id.*, 2:62-3:4, 3:64-4:23; 4:43-5:39; *Decl.* ¶¶70, 73-75. “This data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.” *Ackroyd*, 2:62-3:4.

This information is collected in an “SQL database maintained by the policy organising server 32” (i.e., *base computer*). *Id.*, 3:60-63. Policy organising server 32 is depicted below in the exemplary computer network, along with a remote client computer:

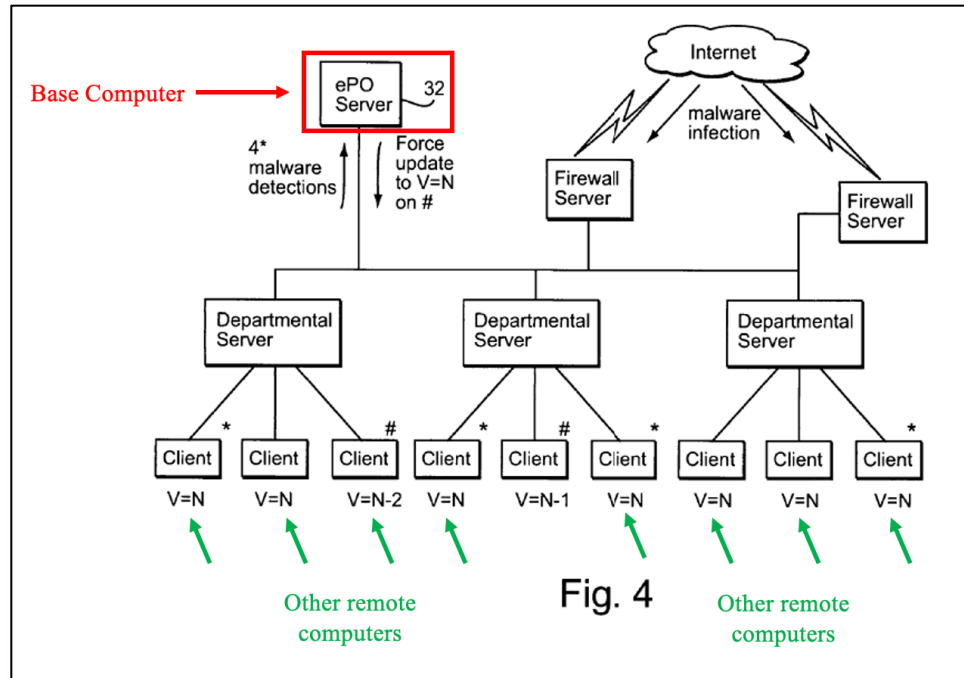


Id., Fig. 4;⁶ see also *id.*, Figs. 1-3, 5-7.

[1(b)] receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;

Like the limitation immediately above, *Ackroyd* also discloses receiving this status information from other remote computers in communication with the base computer in a computer network. *Supra*, Claim 1(a). This is depicted below in Figure 4:

⁶ All annotations added.



Id., Fig. 4 (showing multiple client computers). Once again, the status information received by the base computer includes: **“the malware scanner products being used, the versions of the scanner engines and malware definition data being used, the security settings in force on the computer and the like.”** *Id.*, 2:62-3:4 (emphasis added); see also *id.*, 3:40-54; 3:64-4:23; 4:43-5:39.

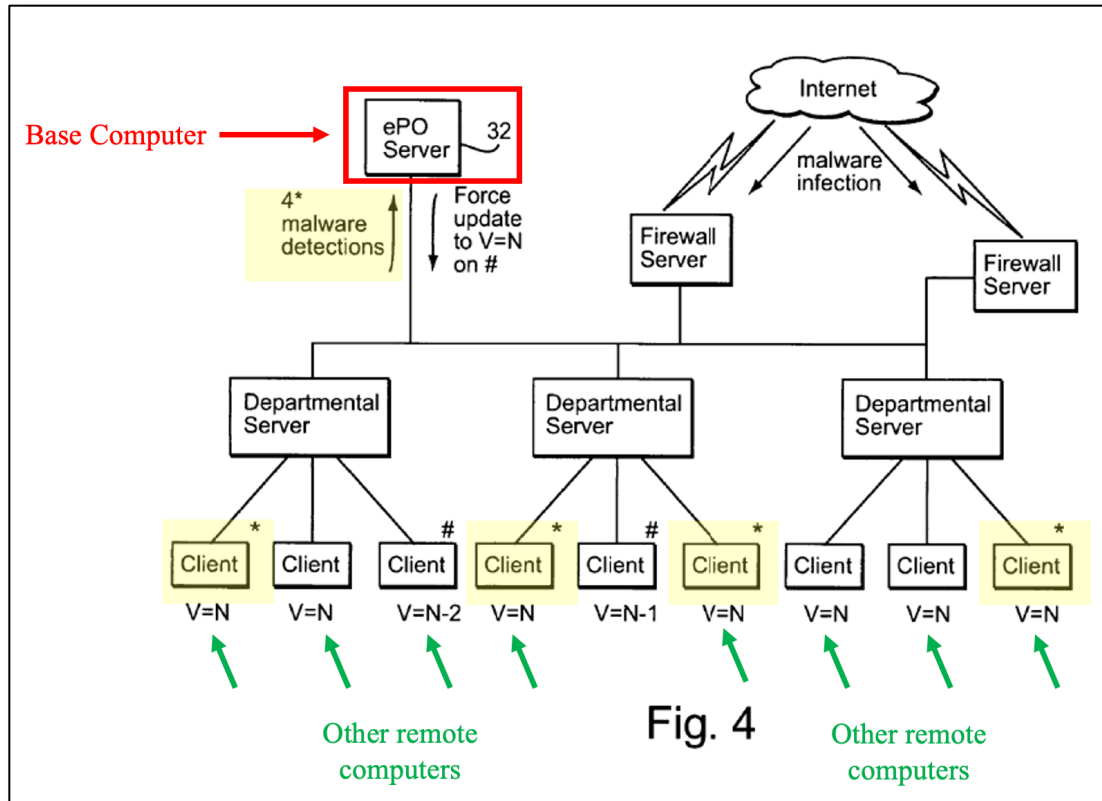
[1(c)] receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;

Ackroyd discloses that the policy organising server receives additional information from at least one of the other remote computers (e.g., client computer V=N with up-to-date malware definition data), including a malware detection event which identifies a detected malware process. From this reported information, the policy organising server determines that the same malware process has been

executed by at least one of the other remote computers (e.g., client computer V=N-2 with outdated malware definition data).

For instance, to detect malware events, *Ackroyd* discloses that “[i]n preferred embodiments of the invention, the network connected computers will typically run their own malware scanners and these malware scanners will preferably use malware definition data to identify the items of malware to be detected.” *Id.*, 2:36-40. In an example, the malware scanners “detect a particular Trojan infection and make reports of this to the policy organising server 32.” *Id.*, 5:26-29; *see also id.*, 4:39-60 (discussing process for malware detection of a “malware infection [] received into the network from the internet” that is “spread within the computer network”), 4:65-67 (detecting “occurrences of internet traffic infected with a particular item of malware”), 5:7-9 (describing detection of malware-related “events”), Fig. 2 (depicting detection and logging of malware events).

After malware is detected by certain client computers, *Ackroyd* discloses that “[t]he policy organising server 32” “serves to receive logged data messages from the various different servers and client computers within the computer network 2 indicating detection of malware items by the malware scanners operating at those individual computers.” *Ackroyd*, 3:44-49. Figure 4 below depicts the base computer receiving malware detection data from other remote client computers having up-to-date malware definition data V=N, identified with “*” (highlighted yellow):



Id., Fig. 4.

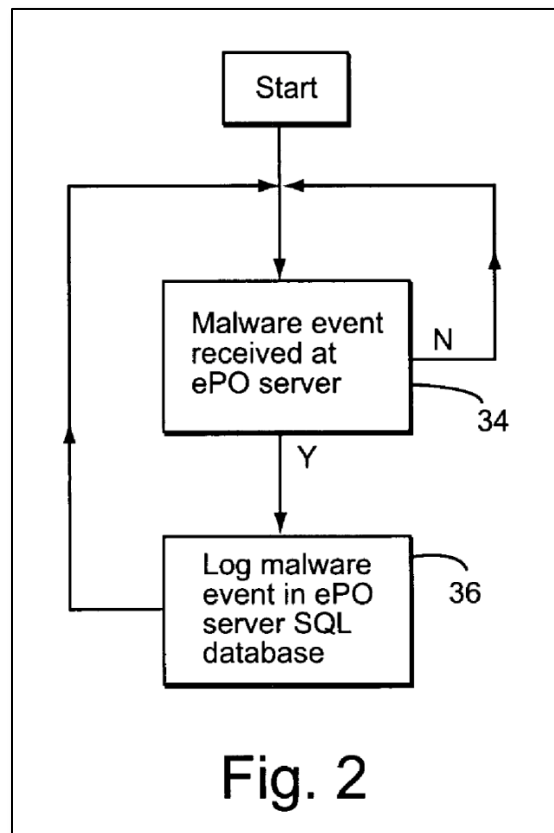
In more detail, with respect to Figure 4, *Ackroyd* discloses that “a malware infection is received into the network from the internet” and “starts to spread within the computer network.” *Id.*, 4:39-42. “Those computers running the most up-to-date version of the virus definition data (indicated by V=N) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32.” *Id.*, 4:43-47. In contrast, “[t]he computers within the network running out-of-date malware definition data (indicated by V=N-1 or V=N-2) do not detect the malware infection and do not give

rise to any logged data messages sent back to the policy organising server.” *Id.*, 4:47-51.

Based on these disclosures, a PHOSITA would have understood or found obvious that *Ackroyd*’s client computers with scanners having up-to-date definition data (e.g., client computers with definition data $V=N$) would identify malware processes and report their associated details to the policy organising server. From the reported information, the policy organising server determines that the same malware process was executed at other remote computers with out-of-date definition data (e.g., client computer with definition data $V=N-2$). *Ackroyd*, 4:47-60 (disclosing that the policy organising server “detects that none of [the event detection messages] originate from a computer running out-of-date malware definition data” and compares received messages to a “predetermined threshold” to force anti-malware actions); *see also*, *Decl.* ¶¶77-85 (noting outdated scanners would not identify malware, and therefore would not trigger anti-malware actions which would allow malware to execute on those client computers with outdated scanners). Client computers with definition data $V=N$ would therefore detect malware starting to spread through the network, such as a Trojan infection, which downloaded to a networked computer with out-of-date definition data and executed potentially malicious processes. *Ackroyd*, 3:44-55 (discussing scanners with updated malware definition data detecting malware processes); *see also*, *Decl.* ¶¶77-85 (noting

“details of the process” includes malware event data associated with the process executing).

As explained above, after detection, this malware event data from an infection spreading through the network is sent to the policy organising server 32. The process is shown below in Figure 2:



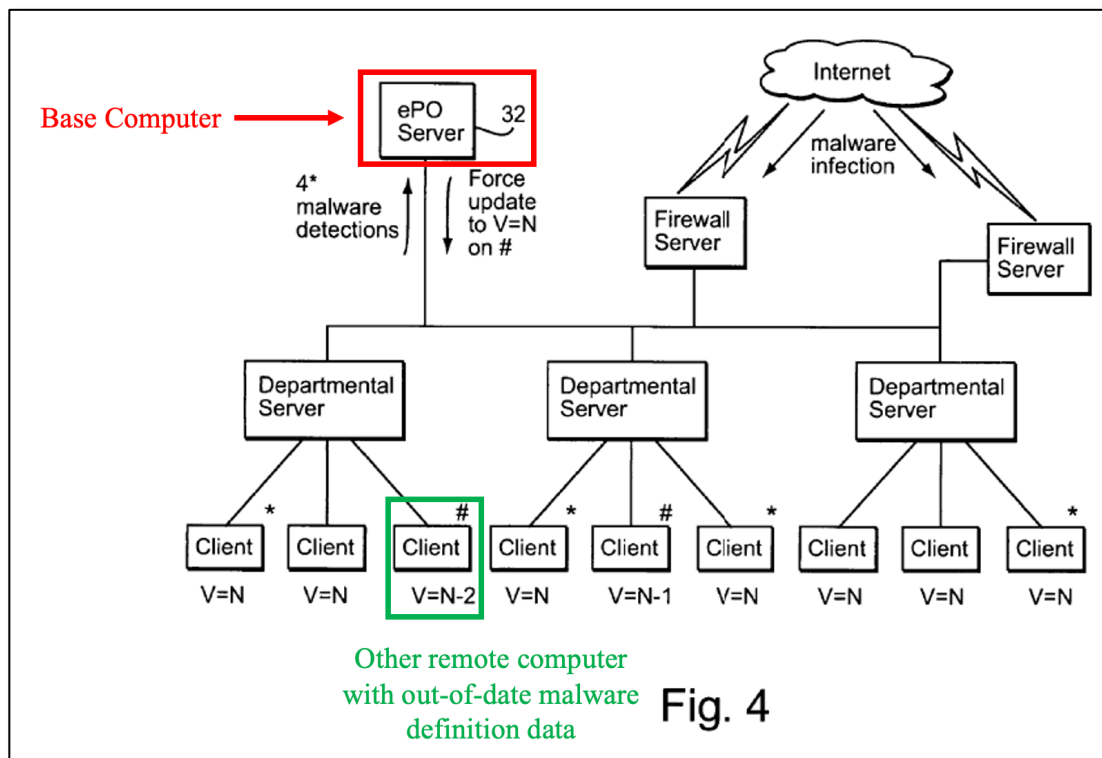
Id., Fig. 2. With respect to Figure 2, *Ackroyd* discloses that:

FIG. 2 illustrates the action of the policy organising server 32 in receiving logged data messages. **At step 34 the policy organising server 32 waits to receive a malware detection event message from one of the various computers it is managing. When such an event is received, processing proceeds to step 36 at which it is logged within an SQL database maintained by the policy organising server 32. Processing then returns to step 36.**

Id., 3:56-63.

[1(d)] determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and

Ackroyd discloses determining that a process is malware not identified by one or more security products on a remote client computer. This process is described with reference to Figure 4, reproduced below:



Ackroyd, Fig. 4.

Ackroyd discloses:

FIG. 4 schematically illustrates a pattern of malware detections and an associated anti-malware action. First of all a malware infection is received into the network from the internet. This starts to spread within the computer network. Those computers running the most up-to-date

version of the virus definition data (indicated by $V=N$) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32. The computers within the network running out-of-date malware definition data (indicated by $V=N-1$ or $V=N-2$) do not detect the malware infection and do not give rise to any logged data messages sent back to the policy organising server. **When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware [identified with “*”] and also detects the pattern that none of these originate from a computer running out-of-date malware definition data [identified with “#”],** the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.

Id., 4:39-60; *see also id.*, 5:7-12 (noting further that malware detection events in excess of a threshold on one scanner with no events on another can “indicate[] that this different malware scanner for some reason is not identifying the malware threat concerned”).

In other words, *Ackroyd’s* “policy organising server” (base computer) receives logged data messages from remote client computer $V=N$ with details of processes executed by remote client computers $V=N-1/V=N-2$ with out-of-date malware definition data (i.e., *the received details of the process that has been executed by the least one of the other remote computers*); determines these processes were not detected by remote client computers $V=N-1$ and $V=N-2$ with out-of-date malware definition data (i.e., *not identified by the one or more security products operating on the at least one of the other remote computers*); and determines these

processes are malware based on the received data (i.e., *determining, by the base computer and based on the received details...that the process is a malware process*). See *id.*; see also *id.*, 4:61-5:12 (describing the process in the context of a firewall server); 5:26-39 (describing the process in the context of isolating a departmental server and related remote computers); Figs. 5-6. To make this malware determination, the policy organising server generates reports from the malware event data, compares these reports to thresholds, and if a threshold is exceeded, initiates predefined anti-malware actions. *Id.*, 3:64-4:38, Fig. 3; *Decl.* ¶¶86-88.

[1(e)] determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer.

As described above, *Ackroyd* discloses that the policy organising server determines that remote computers with out-of-date security products are in fact vulnerable to a specific malware process. This determination is based on an overall assessment of the network, including computers with up-to-date security products and one or more computers with the same or similar vulnerability due to out-of-date security products.

For example, *Ackroyd* discloses:

FIG. 4 schematically illustrates a pattern of malware detections and an associated anti-malware action. First of all a malware infection is received into the network from the internet. This starts to spread within the computer network. Those computers running the most up-to-date

version of the virus definition data (indicated by $V=N$) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32. **The computers within the network running out-of-date malware definition data (indicated by $V=N-1$ or $V=N-2$) do not detect the malware infection and do not give rise to any logged data messages sent back to the policy organising server.** When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware and also detects the pattern that none of these originate from a computer running out-of-date malware definition data, the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to **force the anti-malware action of updating the malware definition data on those computers that are out-of-date.**

Id., 4:39-60. Here, the policy organising server determines that the remote computer (client computer $V=N-1$) is vulnerable to this malware process based on having out-of-date malware definition data, just like other remote client computer $V=N-2$ which also has out-of-date malware definition data, and both of which did not detect a malware event. *Decl.* ¶¶89-91.

Based on this vulnerability determination, *Ackroyd* describes forcing an update of the security products on the vulnerable computers. *Id.*; *see also id.*, 4:61-5:12 (describing the process in the context of a firewall server); 5:26-39 (describing the process in the context of isolating a departmental server and related remote computers); Figs. 4-6.

2. Claim 3

3. The method according to claim 1, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.

Ackroyd discloses the method of claim 1. *Supra*, Claim 1. *Ackroyd* also discloses that:

The database may also advantageously store other information concerning the computers within the computer network relating to their malware protection, such as the malware scanner products being used, the versions of the scanner engines and malware definition data being used, the security settings in force on the computer and the like. This data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.

Ackroyd, 2:62-3:4; *see also id.*, Claim 8 (noting that the database includes, among other things, “malware protection mechanisms[,]” “versions of malware protection[,]” versions of malware definition data[,]” and “security settings of malware protection mechanisms . . .”). To the extent Patent Owner argues that *Ackroyd* does not use the word “name” or the words “signature files,” a PHOSITA would have understood that information about the malware scanner products would include the name of those products. *Decl.*, ¶¶92-94. Likewise, a PHOSITA would have understood that the virus/malware definition data disclosed in *Ackroyd* would include signature file information. *Id.* (explaining that “versions of malware definition data” includes signature file data).

3. Claim 4

4[Pre]. An apparatus comprising:

Ackroyd describes systems and methods for managing malware protection in a computer network. *Supra*, Claim 1[Pre]; *Ackroyd*, claim 22 (“**Apparatus** for managing malware protection...”).

[4(a)] a base computer constructed and arranged to receive details uniquely identifying one or more security products operating at a point in time on a remote computer;

Supra, Claim 1(a).

[4(b)] the base computer being constructed and arranged to receive details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;

Supra, Claim 1(b).

[4(c)] the base computer being constructed and arranged to receive details of a process that has been executed by at least one of the other remote computers;

Supra, Claim 1(c).

[4(d)] the base computer being constructed and arranged to determine, based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and

Supra, Claim 1(d).

[4(e)] the base computer being constructed and arranged to determine that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computers.

Supra, Claim 1(e).

4. Claim 6

6. *The apparatus according to claim 4, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.*

Supra, Claim 3.

5. Claim 7

7. *A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 1.*

Ackroyd discloses the method of Claim 1. *Supra*, Claim 1. *Ackroyd* also discloses “[a] program stored on a computer-readable medium” for conducting its described methods. *Ackroyd*, claim 1; *see also id.*, 5:48-52 (a “central processing unit 202 [that] will execute computer program instructions that may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210...”).

6. Claim 8

8. *A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 2.*

Ackroyd discloses the method of Claim 2. *Supra*, Claim 2. *Ackroyd* also discloses “[a] program stored on a computer-readable medium” for conducting its described methods. *Supra*, Claim 7.

7. Claim 9

9. A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 3.

Ackroyd discloses the method of Claim 3. *Supra*, Claim 3. *Ackroyd* also discloses “[a] program stored on a computer-readable medium” for conducting its described methods. *Supra*, Claim 7.

8. Claim 10

10. The method according to claim 3, wherein the details of all or selected security products further includes settings at a particular point in time.

Ackroyd discloses the method of Claim 3. *Supra*, Claim 3. As described above, *Ackroyd* discloses that:

The database may also advantageously store other information concerning the computers within the computer network relating to their malware protection, such as the malware scanner products being used, the versions of the scanner engines and malware definition data being used, **the security settings in force on the computer and the like**. This data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.

Ackroyd, 2:62-3:4, claim 8 (claiming “security settings of malware protection mechanisms used by respective network connected computers” stored in the database). A PHOSITA would have understood the security settings stored with respect to the client computers “in force on the computer” relates to settings at a particular point in time, namely, the point in time that information was sent. *Decl.*,

¶95.

9. Claim 11

11. The method according to claim 1, further comprising: identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers; and determining, by the base computer, that the identified one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers is vulnerable to the malware process.

Ackroyd discloses the method of Claim 1. *Supra*, Claim 1. Furthermore, referencing Figure 4 above, *Ackroyd* discloses that the policy organising server 32 detects “four logged data messages corresponding to the particular item of malware” and also detects “that none of these originate from a computer running out-of-date malware definition data[,]” such as client computers running software V=N-1 and V=N-2. *Ackroyd*, 4:43-60. Therefore, the policy organising server identifies that V=N-1 and V=N-2, the two remote computers which did not detect the malware event, have similar out-of-date software. *Id.*; *Decl.*, ¶96. Then, “the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.” *Id.*, 4:43-60. In this way, the policy organising server determines that each of client computers running software V=N-1 and V=N-2 are vulnerable to the malware process and prompts an update to resolve this vulnerability. *Decl.*, ¶96 (noting the

system is aware of the security products operating on the remote computers, and the system can also determine vulnerabilities based on this information, such as old versions of malware detection data not identifying a malware infection affecting the network).

10. Claim 12

12. The apparatus according to claim 6, wherein the details of all or selected security products further includes settings at a point in time.

Supra, claim 6; claim 10.

11. Claim 13

13[Pre]. A method comprising:

Ackroyd describes systems and methods for managing malware protection in a computer network. *Supra*, Claim 1[Pre].

[13(a)] receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;

Supra, Claim 1(a).

[13(b)] receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;

Supra, Claim 1(b).

[13(c)] receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;

Supra, Claim 1(c).

[13(d)] determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process;

Supra, Claim 1(d).

[13(e)] determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer;

Supra, Claim 1(e).

[13(f)] identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products and settings as the combination of security products operating on the remote computer; and

Supra, Claim 11.

[13(g)] identifying, by the base computer, one or more malware processes that were not identified by the combination of security products and settings operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.

Ackroyd discloses that its policy organising server identifies one or more malware processes, and also identifies that these one or more malware processes were not identified by remote computers that were running out-of-date malware definition data. *See, e.g., Ackroyd*, 4:39-60:

FIG. 4 schematically illustrates a pattern of malware detections and an associated anti-malware action. First of all a malware infection is received into the network from the internet. This starts to spread within the computer network. Those computers running the most up-to-date version of the virus definition data (indicated by V=N) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32. The computers within the network running out-of-date malware definition data (indicated by V=N-1 or V=N-2) do not detect the malware infection and do not give rise to any logged data messages

sent back to the policy organising server. **When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware and also detects the pattern that none of these originate from a computer running out-of-date malware definition data**, the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.

See also id., Fig. 4.

12. Claim 14

14. The method according to claim 1, wherein the one or more security products include a firewall product and an antivirus product.

Ackroyd discloses the method of Claim 1. *Supra*, Claim 1. Additionally, *Ackroyd* discloses that its malware detection products, e.g., scanners, can include “internet traffic scanning” and can detect “Trojan[s].” *See, e.g., Ackroyd* 2:45-49, 5:26-29 (describing scanner detecting a “Trojan”). It was well-known that firewall products conduct internet traffic scans and detect Trojans. *Decl.*, ¶¶97-98. Therefore, a PHOSITA would have understood or found obvious that *Ackroyd*’s scanners employ a known in the art firewall product to accomplish these functions. *Id.* (describing motivation and reasonable expectation of success); *see also, Ackroyd*, claim 4 (noting these scanners can be “alter[ed]” to “perform[] more thorough malware scanning”). Moreover, *Ackroyd* discloses its “invention relates to the field of malware protection, such as, for example, protection against computer viruses” *Ackroyd*, 1:8-10, 1:59-2:35 (describing “anti-malware” products in the context

of computer viruses), 4:39-60 (same). A PHOSITA would have understood or found obvious that the scanners would additionally include an antivirus product to protect against computer viruses as disclosed in *Ackroyd. Decl.*, ¶¶99-100.

13. Claim 15

15. The apparatus according to claim 4, wherein the one or more security products include a firewall product and an antivirus product.

Supra, Claim 14.

14. Claim 16

16[Pre]. A method comprising:

Supra, Claim 1[Pre].

[16(a)] receiving, at a base computer, details of one or more security products operating at a point in time on a remote computer;

Supra, Claim 1(a).

[16(b)] receiving, at the base computer, details of one or more security products operating on other remote computers in communication with the base computer;

Supra, Claim 1(b).

[16(c)] receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;

Supra, Claim 1(c).

[16(d)] determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process;

Supra, Claim 1(d).

[16(e)] determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of

the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer;

Supra, Claim 1(e).

[16(f)] identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products and settings as the combination of security products operating on the remote computer; and

Supra, Claim 11.

[16(g)] identifying, by the base computer, one or more malware processes that were not identified by the combination of security products and settings operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.

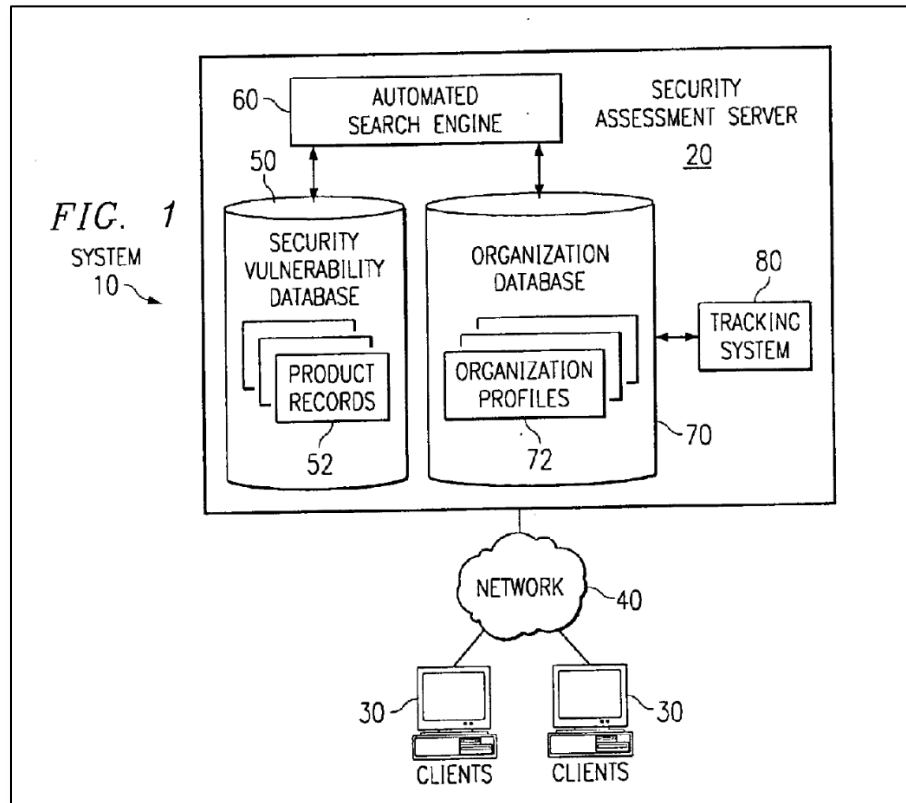
Supra, Claim 13(g).

B. Ground 2: *Ackroyd* in View of *Dahlstrom* Renders Claims 2 and 5 Obvious

Overview of Dahlstrom

Dahlstrom was filed on July 2, 2002 and published on January 8, 2004. *Dahlstrom* therefore qualifies as prior art to the '123 Patent based on 35 U.S.C. § 102(a), (b), and (e). In general, *Dahlstrom* teaches “[a] method for determining security vulnerabilities [that] includes receiving a profile of one or more products used by an organization, the profile including characteristics of each product.” *Dahlstrom*, Abstract. “The method further includes comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more

fixes associated with each security vulnerability.” *Id.* *Dahlstrom*’s system which performs its disclosed methods is depicted below:



Id., Fig. 1. In embodiments, the security vulnerability database includes various information about security products used in a network, such that the database can be used to determine vulnerabilities specific to a particular product and to recommend fixes. *Id.*, [0036]-[0073], Figs. 2-10.

Dahlstrom is analogous art to the ’123 Patent. First, *Dahlstrom* is in the same field of endeavor as the ’123 Patent. For instance, the ’123 Patent states that “[t]he present invention relates generally to methods and apparatus for dealing with malware.” ’123 Patent, 1:9-10. Further, in the ’123 Patent, “[t]he term ‘malware’ is

used herein to refer generally to any executable computer file or, more generally ‘object’, that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.” *Id.*, 1:19-22. Likewise, *Dahlstrom* is in the same field of endeavor, and describes its field of invention as follows: “[t]his invention relates in general to the field of information technology, and more particularly to a system and method for determining security vulnerabilities.” *Dahlstrom*, [0001]; *Decl.*, ¶¶64-67 (noting *Dahlstrom* was found analogous by the Examiner and applied in rejections in U.S. prosecution).

Second, *Dahlstrom* is reasonably pertinent to a problem identified and purportedly solved by the ’123 Patent. The ’123 Patent describes a problem with existing malware detection as being slow to respond to new forms of malware, particularly in a network of remote computers. *See* ’123 Patent, 2:23-47 (describing existing malware products); 3:14-24 (describing the claimed invention as different from the prior art, and noting that the methods in the ’123 Patent allow “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. Sophisticated pattern analysis can be carried out. This allows a rapid determination of the nature of the object to be made....”). Likewise, *Dahlstrom* teaches a solution to the same problem. *See Dahlstrom*, [0003] (describing the problem and noting that “organizations are perhaps less prepared

than ever to monitor and prevent security vulnerabilities. This is due to both the sheer volume of products and the rate at which new products are introduced and/or existing products modified. Adding to the difficulty of such monitoring and prevention, organizations have also become much more distributed geographically . . .”), [0006] (describing the solution, in part, as “comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more fixes associated with each security vulnerability.”); *Decl.*, ¶¶64-67. Because *Dahlstrom* is in the same field of endeavor as the ’123 Patent, and additionally and separately because *Dahlstrom* is reasonably pertinent to a problem the ’123 Patent purports to solve, *Dahlstrom* is analogous art to the ’123 Patent for purposes of prior art analysis under 35 U.S.C. § 103.

1. Claim 2

2. The method according to claim 1, further comprising: providing information to the user of the remote computer that the remote computer may be susceptible to attack by the malware processes.

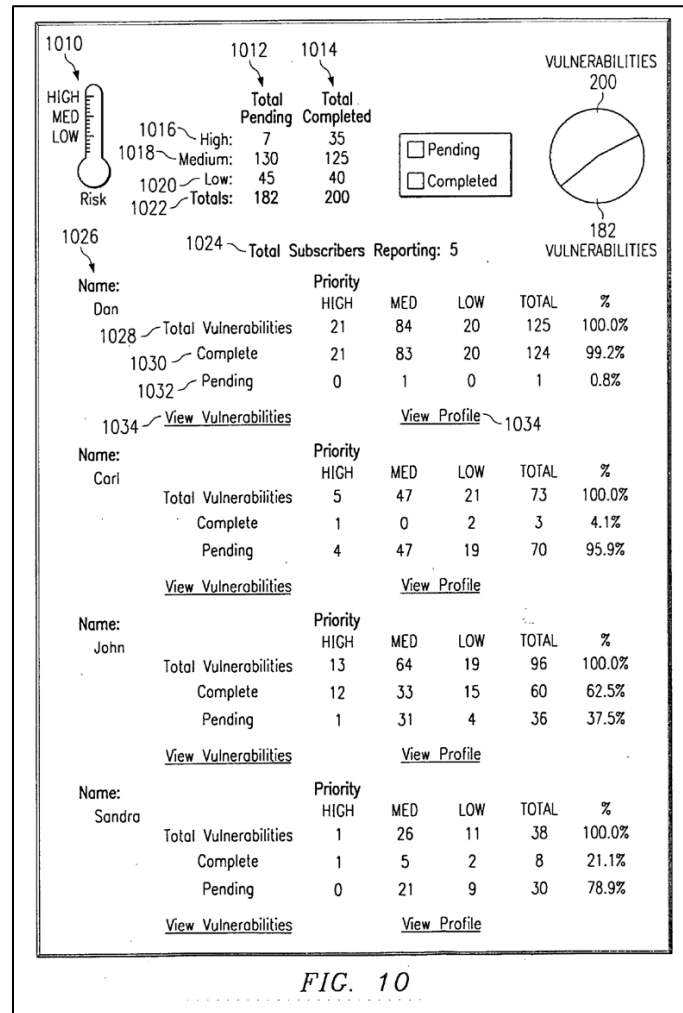
Ackroyd discloses the method of Claim 1. *Supra*, Claim 1. Further, *Ackroyd* generally discloses “[t]he results of the processing performed” related to malware and vulnerability determinations “may be **displayed to a user** via the display driver 212 and the monitor 214.” *Ackroyd*, 5:52-54; *see also id.*, 3:64-4:13 (disclosing the system will “run various queries/**reports** (these terms are used generically to

indicate mechanisms for retrieving specified data from a database and **presenting it to a user** rather than implying the use of any particular software or display/data format)...”). In view of this, a PHOSITA would have understood *Ackroyd* teaches that information is provided to the user of a remote computer that the computer may be susceptible to attack. *Decl.*, ¶101.

Nevertheless, the analysis provided by the EPO indicates that the examining body found *Ackroyd*’s teachings here unconvincing. To the extent the Board finds that the express teachings of *Ackroyd* are insufficient, it would have been obvious to combine *Ackroyd* with *Dahlstrom* to render this claim obvious.

Dahlstrom discloses “a tracking report generated by the tracking system 80[,]” which includes both a risk thermometer and also “vulnerability tracking categories of 1012 and 1014, corresponding to pending vulnerabilities that have not been neutralized or otherwise addressed and completed vulnerabilities that have been neutralized or otherwise addressed, respectively.” *Dahlstrom*, [0071]. *Dahlstrom* also explains that “[t]he tracking report [] breaks down the overall vulnerabilities of an organization into vulnerabilities under the scope or direction of individuals or subscribers within the organization.” *Id.*, [0072]. That way, “a supervisor or IT manager can easily access, monitor, and track the efforts of individuals within an organization to neutralize or otherwise address vulnerabilities.” *Id.* As described in *Dahlstrom*, these tracking reports and other risk assessments can be retrieved from,

and provided to, the user of the remote computer. *See, e.g., id.*, [0019], [0021], [0037]-[0038], [0049]-[0052]. An example of a tracking report in *Dahlstrom* is shown below at Figure 10:



Dahlstrom, Fig. 10.

It would have been obvious for a PHOSITA to incorporate vulnerability data associated with certain product configurations outlined in the tracking report disclosed in *Dahlstrom* with the report disclosed in *Ackroyd* that is already being presented to the user. *Decl.*, ¶¶102-105. *Dahlstrom* expressly includes more

implementation details, but the concepts from the two references are the same—information about the network and its exposure to possible malware is communicated to users. *Id.* A PHOSITA would have been motivated to make this combination because the implementation details described and illustrated in the tracking report from *Dahlstrom* would be useful in communicating the necessary information from the system processing that is described in *Ackroyd*. *Id.* There is express motivation in the references themselves for this combination. For instance, *Ackroyd* describes determining that a computer is vulnerable to a malware attack. *See, e.g., Ackroyd*, 4:43-60. And *Ackroyd* describes communicating this information to a user. *See, e.g., id.*, 5:52-54. Further, *Ackroyd* discloses that its reports “may be configured and enhanced by individual users to tailor them to their particular networks[.]” *Id.*, 4:9-17. Thus, it would have been obvious to a PHOSITA to implement this communication to the user by using the format for vulnerability data in the tracking report described in *Dahlstrom*, which includes information about various vulnerabilities. *Decl.*, ¶¶102-105. This is an obvious design choice, and would accomplish the goals that are already described in *Ackroyd*, and a PHOSITA would have appreciated success making this simple modification. *Id.*

2. Claim 5

5. The apparatus according to claim 4, wherein the base computer is constructed and arranged to provide information to the user of the remote computer that the remote computer may be susceptible to attack by the malware process.

Supra, Claim 2.

V. DISCRETIONARY DENIAL IS NOT WARRANTED

A. The *Advanced Bionics* Framework Favors Institution Under § 325(d)

Under the two-part *Advanced Bionics* framework applying the *Becton, Dickinson* factors, the Board should not exercise its discretion to deny institution under 35 U.S.C. § 325(d).

Part one considers whether the same or substantially the same prior art or arguments were previously presented to the office. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (Feb. 13, 2020); *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8, 17-18 (Dec. 15, 2017). Petitioner presents two new grounds of unpatentability. Petitioner’s first ground relies on a prior art reference, *Ackroyd*, that was submitted late in the process during initial examination and was not used in any rejection during U.S. prosecution. As this Board has previously found in two related proceedings, when a reference was not applied in a rejection during U.S. Prosecution, the Board “cannot determine the extent to which [the reference] was evaluated during the examination[.]” *CrowdStrike, Inc. v. Webroot Inc.*, IPR2023-00126, Paper 9, at 14 (PTAB May 5, 2023); *see also CrowdStrike, Inc. v. Open Text Inc.*, IPR2023-00124,

Paper 11, at 17 (PTAB June. 15, 2023) (“the extent to which [the reference] was evaluated during prosecution for the [Challenged Patent] is unclear because [the reference] was never used in a rejection”).

In the related IPR2023-00126 proceeding, the reference at issue (*Morris*) had been mapped against claims similar to those challenged in the IPR. An International Search Report, including the *Morris* mapping, was submitted during U.S. Prosecution. Yet the Board in IPR2023-00126 still declined to find the first *Advanced Bionics* factor satisfied because there was no discussion by the U.S. Examiner. The Board found the same in IPR2023-00124. Notably, here, the Examiner was given even less detail on *Ackroyd*’s teachings via submission of a European Search Report. Indeed, *Ackroyd* was submitted during U.S. Prosecution in a European Search Report that merely identified the reference as relevant, but did not map its teachings to any claim limitations. Ex. 1003 (EPO FH), 167-171. Accordingly, as in the related proceedings, “because [*Ackroyd*] was not the basis of a rejection,” there is not “enough similarity and overlap to move to the second step of the *Advanced Bionics* framework[.]” IPR2023-00126, Paper 9, at 14; *see also* IPR2023-00124, Paper 11, at 17.

To the extent the Board reaches step two, for the reasons presented in the Petition and for the same reasons the EPO Examiner found *Ackroyd* “very relevant for the present invention,” and ultimately rejected the EPO claims, the U.S.

Examiner erred during examination justifying reconsideration of the Challenged Claims in view of *Ackroyd. DJI Europe B.V. v. Textron Innovations Inc.*, IPR2022-00453, Paper 10 at 11-13 (PTAB Aug. 3, 2022) (finding error where examiner did not consider relevance of prior art addressed in EPO office action).

Petitioner's second ground relies on *Ackroyd* (discussed above) in view of *Dahlstrom*. While *Dahlstrom* was applied in rejections during U.S. prosecution, (1) errors during prosecution evidence that the issued claims may not be patentable over *Dahlstrom* and (2) Petitioner's application of *Dahlstrom* is markedly different than was presented previously to the Examiner.

Namely, during prosecution, *Dahlstrom* was proposed as a primary reference in combination with *Beddoe* to reject the then-pending claims. As discussed above, Applicant distinguished *Dahlstrom* in view of the prior art of record, relying on the subject matter of then-pending claim 3 involving "security products on multiple computers scanning remote computers, detecti[ng] malware in cloud by remote and base computers" and discussing amending the independent claims to include this concept. *No such amendment was ever entered*. Instead, the Examiner included an Examiner's Amendment with the Notice of Allowability, and that amendment required: "receiving, at a base computer, details uniquely identifying one or more security products...." As described in more detail above, the Reasons for Allowance also cited to a limitation **not present** in the issued claims: "Detecting malware on

remote computers by base computer, by comparing the security product(s) on remote and base computers, and comparing malware objects by size, name, logical storage and path of the malware object and details as described in the independent claim(s).”

As to these limitations, which the Examiner stated were reasons for allowance but were not included in the as-issued claims, there is no evidence the Examiner applied *Dahlstrom*’s teachings to the as-issued claims, nor to these purported concepts missing in the claims.

Either way, Petitioner proposes *Dahlstrom* in a markedly different way as a secondary in combination with *Ackroyd*. Petitioner relies on *Ackroyd*’s teachings for the purportedly patentable “receiving, at a base computer, details uniquely identifying one or more security products...” limitation. The same or substantially the same arguments were therefore not presented during prosecution. Additionally, should the Board find the same or similar arguments were at issue, the Examiner clearly erred both by issuing the claims without the requisite amendments, and by not considering the teachings of *Dahlstrom* in combination with *Ackroyd*.

B. The *Fintiv* Factors Favor Institution

Under the “*Fintiv* factors,” the Board may consider parallel litigation, including an early trial date, in determining whether to institute under 35 U.S.C. § 314(a). *NHK Spring Co., Ltd., v. Intri-Plex Technologies, Inc.*, IPR2018-00752, Paper 8 at 19–20 (PTAB Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv, Inc.*,

IPR2020-00019, Paper 11 at 2–3, 6 (PTAB Mar. 20, 2020) (precedential). Those factors favor institution here.

1. Stay

Parallel litigation is ongoing. While no stay has been requested, Petitioner may seek a stay if institution is granted, thus favoring institution. At worst, this factor is neutral because the Board “will not attempt to predict” how the district court will proceed. *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB Jun. 16, 2020).

2. Proximity of the Court’s Trial Date

“This factor looks at the proximity of the trial date to the date of [FWD] to assess the weight to be accorded a trial date set earlier than the expected [FWD] date.” *Shenzhen Carku Tech. Co., Ltd. v. The Noco Co.*, IPR2020-00944, Paper 20 at 61 (PTAB Nov. 12, 2020). Understanding “scheduled trial dates are unreliable and often change,” recent Interim *Fintiv* Guidance⁷ dictates “[a] court’s scheduled trial date...is not by itself a good indicator of whether the district court trial will occur before the statutory deadline for a [FWD].” *Samsung Elec.’s Co., Ltd. et al. v.*

⁷https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621.pdf (“Interim *Fintiv* Guidance”).

Staton Techiya, LLC, IPR2022-00302, Paper 13, at 10 (PTAB July 11, 2022). When analyzing this factor, “the parties [may] rely on time-to-trial statistics” along with “additional supporting factors such as the number of cases before the judge in the parallel litigation and the speed and availability of other case dispositions.” *Id.*, 10-12 (“In weighing factor two, we follow the Interim *Fintiv* Guidance”).

Based on the most recent WDTX statistics, the “actual trial date” is likely to be held mid-January, 2025—28.3 months from September 8, 2022, the date the first Amended Complaint was filed asserting the ’123 Patent against CrowdStrike.⁸ While the District Court entered a schedule with an August 19, 2024 trial date assigned to each defendant in five separate lawsuits that have been consolidated for pretrial issues, PO has admitted that “median time-to-trial statistics are more appropriate” for consideration under this factor. IPR2023-00289, Paper 6, at 13; *Amendment to Scheduling Order* (Dkt. 252, Ex. 1007), 8. Either way, because the court’s consolidation is limited to pretrial issues, separate trials will be required, and trial cannot proceed on August 19, 2024 for all defendants.

The Board’s FWD deadline in this case is expected in January or early February 2024, potentially before or commensurate with when a trial would occur

⁸https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0630.2022_0.pdf (June 30, 2022, 28.3 months for median time-to-trial in WDTX).

based on the time-to-trial statistics this Board should apply to its analysis. However, “additional supporting factors” are at play weighing towards a longer than average filing-to-trial window. First, the District Court litigation involves thirty-nine total patents, including twelve asserted by Patent Owner against Petitioner and two counterclaim infringement allegations brought by Petitioner. As PO previously quoted, U.S. Magistrate Judge Gilliland explained in a December 9, 2022 hearing that this is “a phenomenal case that I’m hoping one day maybe people will write songs about because it is about as complicated as you’re going to get with patent cases.” IPR2023-00289, Paper 6, at 2.

To accommodate the significant number of allegations, the Court scheduled three Markman hearings, the first was conducted on March 7, 2023, the second was recently held on May 3, 2023 relating to the Counterclaim patents, and the final Markman is scheduled for July 25, 2023, which will involve the Challenged Patent. *Amendment to Scheduling Order* (Dkt. 252, Ex. 1007), 3, 5, 6. Accordingly, with multiple Markman hearings and a multitude of claims involved in a phenomenally complex case, the “actual trial date” is much more likely to be delayed until later, commensurate with the median time to trial (or later) and after FWD here.

Moreover, the ’123 Patent was added to the litigation in September 2022 as one of six additional asserted patents, introduced over six months after the original six patents were asserted against Petitioner. The ’123 Patent, and other late asserted

patents, were shoehorned into an already ongoing litigation, resulting in a shortened window to trial. Petitioner acted diligently in filing its Petition against this newly asserted patent, and any shortened window to trial for these patents is the result of PO's own litigation strategy.

In sum, the Board's FWD deadline in this case falls either **before** or commensurate with when a trial would occur based on WDTX time-to-trial statistics. But the additional complicating factors at issue here suggest trial will occur even later in time than the statistics suggest, weighing heavily in favor of institution.

3. Investment in Parallel Proceeding

Beyond claim construction, the parties have invested little in the parallel proceeding. The first and second *Markman* hearings were just recently conducted on March 7, 2023 and May 3, 2023, respectively. The final *Markman* is not scheduled until July 25, 2023. Fact discovery just opened on April 18, 2023 and is not set to conclude until January 18, 2024. Expert discovery does not close until March 12, 2024 and dispositive motions are not due until May 7, 2024. This factor weighs in favor of institution.

4. Overlap

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 '123 Patent that utilizes *Ackroyd* or *Dahlstrom*—the prior art references relied upon in the

grounds of the instant petition. Petitioner’s proposal is comprehensive and addresses the concern of narrowing the issues, as this stipulation ensures there is no overlap between the ’123 Patent invalidity theories before the Board and at issue in the District Court. Petitioner’s proposed stipulation is far more restrictive than a *Sand Revolution* stipulation, which excludes only the same grounds advanced in the IPR, allowing the Petitioner to rely on the same references in the two tribunals so long as the reliance is not identical. Accordingly, this factor weighs heavily in favor of institution.

5. Same Party

The Parties are the same in the district court litigation. However, members of the Board have noted *Fintiv* addresses only the scenario in which the petitioner is unrelated to a defendant in a parallel proceeding, finding this should weigh against denying institution, but that *Fintiv* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10-11 (PTAB May 15, 2020) (APJ Crumbley, dissenting) (noting that disfavoring a “defendant in the district court” is “contrary to the goal of providing district court litigants an alternative venue to resolve questions of patentability”).

6. Other Circumstances

“[W]here the PTAB determines that the information presented at the institution stage presents a compelling unpatentability challenge, **that determination alone** demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*.” *Hewlett Packard Enterprise Co., et al. v. Biljco LLC*, IPR2022-00420, Paper 17, at 6 (PTAB July 12, 2022) (“[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.”). The strength of Petitioner’s proposed grounds presented above (which the EPO found “very relevant for the present invention” leading to a final rejection) weighs strongly in favor of institution. *Id.* (refusing to deny institution under the *Fintiv* framework based solely on the strength of Petitioner’s grounds).

VI. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz

Adam P. Seitz, Reg. No. 52,206

Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER

VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner and CrowdStrike Holdings, Inc. are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '123 Patent is presently the subject of a patent infringement lawsuit filed against Petitioner in the United States District Court for the Western District of Texas Waco Division. *Webroot, Inc. et al. v. CrowdStrike Holdings, Inc. et al.*, Case No. 6:22-cv-00241. Petitioner understands the '123 Patent has also been asserted in the following matter:

- *Webroot, Inc. et al. v. Sophos Ltd.*, Case No. 6:22-cv-00240 (WDTX).

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Adam P. Seitz (Reg. No. 52,206) Adam.Seitz@eriseip.com PTAB@eriseip.com	Paul R. Hart, (Reg. No. 59,646) Paul.Hart@eriseip.com PTAB@eriseip.com
<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 5299 DTC Blvd., Ste. 1340 Greenwood Village, Colorado 80111 Telephone: (913) 777-5600 Fax: (913) 777-5601

APPENDIX OF EXHIBITS

EX1001	U.S. Patent No. 8,763,123 (“123 <i>Patent</i> ”)
EX1002	File History of U.S. Patent No. 8,763,123 (“123 <i>FH</i> ”)
EX1003	European File History (“ <i>EPO File History</i> ”)
EX1004	Declaration of Markus Jakobsson, Ph.D. (“ <i>Dec.</i> ”)
EX1005	U.S. Patent No. 7,269,851 to Ackroyd (“ <i>Ackroyd</i> ”)
EX1006	U.S. Patent Publication No. 2004/000670 to Dahlstrom et al. (“ <i>Dahlstrom</i> ”)
EX1007	22-cv-00241, Dkt. 252, Order Granting Fifth Amended Scheduling Order (“ <i>Amendment to Scheduling Order</i> ”)
EX1008	22-cv-00241, Dkt. 304, Plaintiffs’ Responsive Claim Construction Brief (“ <i>Responsive Markman Brief</i> ”)
EX1009	U.S. Patent No. 6,944,772 to Dozortsev (“ <i>Dozortsev</i> ”)
EX1010	EP 1,549,012 to De Spiegeleer (“ <i>Spiegeleer</i> ”)
EX1011	EP 1,280,040 to Hinchliffe et al. (“ <i>Hinchliffe</i> ”)
EX1012	WO 2002/033525 to Chuang (“ <i>Chuang</i> ”)
EX1013	U.S. Patent Publication No 2004/0073810 to Dettinger et al. (“ <i>Dettinger</i> ”)
EX1014	WO 2003/021402 to Duke (“ <i>Duke</i> ”)
EX1015	U.S. Patent Publication No 2003/0115479 to Edwards et al. (“ <i>Edwards</i> ”)
EX1016	Intentionally left blank
EX1017	U.S. Patent No. 6,663,000 to Muttik et al. (“ <i>Muttik</i> ”)
EX1018	PC Broadband Security by Darren Meyer (“ <i>PC broadband security</i> ”)
EX1019	Wired to the World Anti-virus Software by Ralph Lee Scott (“ <i>Anti-virus software</i> ”)

CLAIM LISTING APPENDIX

U.S. Patent No. 8,763,123, Claims 1-16

Claim Designation	Claim Language
Claim 1[P]	A method comprising:
Claim [1(a)]	receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;
Claim [1(b)]	receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;
Claim [1(c)]	receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;
Claim [1(d)]	determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and
Claim [1(e)]	determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer.
Claim 2	The method according to claim 1, further comprising: providing information to the user of the remote computer that the remote computer may be susceptible to attack by the malware processes.
Claim 3	The method according to claim 1, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.
Claim 4[P]	An apparatus comprising:
Claim [4(a)]	a base computer constructed and arranged to receive details uniquely identifying one or more security products operating at a point in time on a remote computer;
Claim [4(b)]	the base computer being constructed and arranged to receive details uniquely identifying one or more security products

	operating on other remote computers in communication with the base computer;
Claim [4(c)]	the base computer being constructed and arranged to receive details of a process that has been executed by at least one of the other remote computers;
Claim [4(d)]	the base computer being constructed and arranged to determine, based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and
Claim [4(e)]	the base computer being constructed and arranged to determine that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computers.
Claim 5	The apparatus according to claim 5, wherein the base computer is constructed and arranged to provide information to the user of the remote computer that the remote computer may be susceptible to attack by the malware process.
Claim 6	The apparatus according to claim 4, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.
Claim 7	A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 1.
Claim 8	A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 2.
Claim 9	A computer program recorded on a non-transitory computer readable medium comprising program instructions for causing a computer to perform a method according to claim 3.
Claim 10	The method according to claim 3, wherein the details of all or selected security products further includes settings at a particular point in time.
Claim 11	The method according to claim 1, further comprising: identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one

	of the other remote computers; and determining, by the base computer, that the identified one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers is vulnerable to the malware process.
Claim 12	The apparatus according to claim 6, wherein the details of all or selected security products further includes settings at a point in time.
Claim 13[P]	A method comprising:
Claim [13(a)]	receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;
Claim [13(b)]	receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;
Claim [13(c)]	receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;
Claim [13(d)]	determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process;
Claim [13(e)]	determining, by the base computer, that the remote computer is vulnerable to the malware process,
Claim [13(e)(1)]	wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer;
Claim [13(f)]	identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products and settings as the combination of security products operating on the remote computer; and
Claim [13(g)]	identifying, by the base computer, one or more malware processes that were not identified by the combination of security products and settings operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.

Claim 14	The method according to claim 1, wherein the one or more security products include a firewall product and an antivirus product.
Claim 15	The apparatus according to claim 4, wherein the one or more security products include a firewall product and an antivirus product.
Claim 16[P]	A method comprising:
Claim [16(a)]	receiving, at a base computer, details of one or more security products operating at a point in time on a remote computer;
Claim [16(b)]	receiving, at the base computer, details of one or more security products operating on other remote computers in communication with the base computer;
Claim [16(c)]	receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;
Claim [16(d)]	determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process;
Claim [16(e)]	determining, by the base computer, that the remote computer is vulnerable to the malware process,
Claim [16(e)(1)]	wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer;
Claim [16(f)]	identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products and settings as the combination of security products operating on the remote computer; and
Claim [16(g)]	identifying, by the base computer, one or more malware processes that were not identified by the combination of security products and settings operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 11,840 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: July 12, 2023

Respectfully submitted,

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
Adam.Seitz@eriseip.com
Erise IP, P.A.
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105(a)**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on July 12, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '123 patent:

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
United States

Respectfully submitted,

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
Adam.Seitz@eriseip.com
Erise IP, P.A.
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER