

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

FORTINET, INC.,

Petitioner,

v.

NETSKOPE, INC.,

Patent Owner.

---

U.S. Patent No. 8,635,697

Case No.: IPR2026-00031

**PATENT OWNER'S PRELIMINARY RESPONSE**

## TABLE OF CONTENTS

|      |                                                                                                                                                                                                                                                  |    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I.   | INTRODUCTION .....                                                                                                                                                                                                                               | 1  |
| II.  | THE '697 PATENT .....                                                                                                                                                                                                                            | 2  |
| A.   | Brief Description of the '697 Patent .....                                                                                                                                                                                                       | 2  |
| B.   | Independent Claims of the '697 Patent .....                                                                                                                                                                                                      | 6  |
| III. | LEVEL OF ORDINARY SKILL IN THE ART .....                                                                                                                                                                                                         | 7  |
| IV.  | CLAIM CONSTRUCTION .....                                                                                                                                                                                                                         | 7  |
| V.   | OVERVIEW OF REFERENCES USED IN THE PETITION .....                                                                                                                                                                                                | 8  |
| A.   | Overview of Deridder.....                                                                                                                                                                                                                        | 8  |
| B.   | Overview of Tuvell .....                                                                                                                                                                                                                         | 10 |
| C.   | Overview of Lee.....                                                                                                                                                                                                                             | 13 |
| VI.  | THE PETITION FAILS TO SHOW THE CHALLENGED CLAIMS ARE UNPATENTABLE .....                                                                                                                                                                          | 16 |
| A.   | A POSITA Would Not Have Found it Obvious to Combine Deridder with Tuvell and Lee.....                                                                                                                                                            | 16 |
| B.   | The Combination Does Not Teach or Suggest 1[b]’s “ <i>Determining an Operating System Identifier (OS ID) Associated with the TCP Session and the Computing Device</i> ” .....                                                                    | 22 |
| C.   | The Combination Does Not Teach or Suggest Element 1[c]’s “ <i>Determining If Malware Is Present in the TCP Session and an Associated Malware ID by Comparing a Malware Signature to the One Or More TCP Packets</i> ” .....                      | 24 |
| D.   | The Combination Does Not Teach or Suggest Element 1[d]’s “ <i>Generating an Alert Identifying a Network Address Associated with the Access Device, the Malware ID and the OS ID Associated with TCP Session That Generated the Alert</i> ” ..... | 27 |
| E.   | The Combination Fails to Render Obvious Any of the Challenged Claims.....                                                                                                                                                                        | 29 |
| VII. | PETITIONER IMPROPERLY RELIES ON POSITA’S KNOWLEDGE INSTEAD OF DISCLOSURE OR TEACHING IN THE PRIOR ART REFERENCES.....                                                                                                                            | 29 |

|                       |    |
|-----------------------|----|
| VIII. CONCLUSION..... | 33 |
|-----------------------|----|

## **EXHIBIT LIST**

| <b>No.</b>          | <b>Exhibit Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ex. 2001</b>     | U.S. Patent Publication No. 2016/0232349 A1                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Ex. 2002</b>     | File History of U.S. Patent Application No. 14/617,787                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Ex. 2003</b>     | Website blog on Fortinet.com, titled: “Fortinet is Leading Innovation in the Security Industry with More Than 1,500 Patents”<br><a href="https://www.fortinet.com/blog/business-and-technology/fortinet-is-the-security-innovation-leader-more-than-1500-patents-either-awarded-or-pending">https://www.fortinet.com/blog/business-and-technology/fortinet-is-the-security-innovation-leader-more-than-1500-patents-either-awarded-or-pending</a> |
| <b>Ex. 2004</b>     | Website article on Wikipedia.org, titled: “Fortinet”<br><a href="https://en.wikipedia.org/wiki/Fortinet">https://en.wikipedia.org/wiki/Fortinet</a>                                                                                                                                                                                                                                                                                               |
| <b>Ex. 2005</b>     | Fortinet Inc.’s Preliminary Invalidity Contentions in <i>Netskope, Inc. v. Fortinet, Inc.</i> , Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California.                                                                                                                                                                                                                                  |
| <b>Ex. 2006</b>     | Plot from Docket Navigator – Profile of Judge Haywood S. Gilliam<br>Motion Success To Stay Pending IPR                                                                                                                                                                                                                                                                                                                                            |
| <b>Ex. 2007</b>     | Scheduling Order for <i>Netskope, Inc. v. Fortinet, Inc.</i> , Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California                                                                                                                                                                                                                                                                    |
| <b>Ex. 2008</b>     | Plots from Docket Navigator – Profile of Judge Haywood S. Gilliam<br>Time to Milestones (annotated)                                                                                                                                                                                                                                                                                                                                               |
| <b>Ex. 2009</b>     | Part of Fortinet Inc.’s Preliminary Invalidity Contention Charts for ’697 Patent in <i>Netskope, Inc. v. Fortinet, Inc.</i> , Case No. 4:25-cv-02360-HSG, pending in the United States District Court for the Northern District of California.                                                                                                                                                                                                    |
| <b>NEW EXHIBITS</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Ex. 2010</b>     | Declaration of Dr. Michael Franz                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Ex. 2011</b>     | U.S. Patent No. 9,104,871                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>EX. 2012</b>     | U.S. Patent No. 9,009,818                                                                                                                                                                                                                                                                                                                                                                                                                         |

## **I. INTRODUCTION**

Patent Owner Netskope, Inc. ("Patent Owner") respectfully submits this Preliminary Response to the Petition for *Inter Partes Review* ("IPR") filed by Fortinet, Inc. ("Petitioner") challenging claims 1–25 ("Challenged Claims") of U.S. Patent No. 8,635,697 ("the '697 patent") based on a single obviousness ground using a combination of three references—Deridder, Tuvell and Lee.

Petitioner's invalidity ground falls woefully short since the Petition fails to establish that it would have been obvious to combine these three disparate references, and the purported motivations to combine are mere speculations that fail to account for the existing capabilities already described in those references. Furthermore, Deridder, Tuvell and Lee do not individually or collectively disclose, teach, or even suggest each claimed feature and the claimed invention as a whole.

The Petition is also substantively flawed because it impermissibly relies on the knowledge of a person of ordinary skill in the art ("POSITA") for limitations that the Petition's references fall short of disclosing or teaching.

Because the Petition has failed to demonstrate a reasonable likelihood that Petitioner would prevail in showing that any of the Challenged Claims is unpatentable, institution should be denied under 35 U.S.C. § 314.

## **II. THE '697 PATENT**

The '697 patent was filed on April 8, 2011, claiming priority to U.S. Provisional Application No. 61/469,024, filed March 29, 2011. Ex. 1001, front page. Therefore, as acknowledged by Petitioner, the priority date of the claims of the '697 patent is March 29, 2011. Petition, 2.

### **A. Brief Description of the '697 Patent**

The '697 patent relates to malware detection and identification of computers coupled to a service provider network that are infected with malicious software (malware) from session traffic associated with the computers. Ex. 1001, Abstract, 1:16-21. The '697 patent specification explains that residential and business networks are connected to, e.g., the Internet using a gateway or router that uses network address translation (NAT), which “maps local area network (LAN) addresses of multiple devices to a single WAN IP address enabling multiple devices to access the internet using WAN address.” *Id.*, 1:27-30. While each computer within the residential or business network has its own IP address, the NAT device modifies network address information for the purpose of remapping one IP address space into another such that all traffic emerging from the network shares the same IP address that is assigned to the gateway or router. *Id.*, 1:30-45. “This is a particular problem when network based virus or malware detection is utilized where the wide area network WAN IP traffic is analyzed to determine the presence of potential

malware originating from the LAN. The inability to determine a specific device means that any remediation procedures can not be applied in a focused manner.” *Id.*

Notably, the '697 patent explains “[i]n a network-based malware detection system, the ability to identify an operating system enables information to be provided to the user to speed the remediation process. A household with multiple computers, or computing devices, each potentially running different operating systems can require considerable time to remediate. ***The ability to provide identification of an operating system that is infected and request that the user access the remediation portal with a computer that has a particular operating system can improve the results of the remediation process.***” *Id.* 3:18-27 (emphasis added).

To this end, the '697 patent describes methods and devices that not only detect malware but identify the OS information of the infected devices that are behind the NAT device. *Id.*, 3:28-47. This allows OS-specific remediation to be focused on those devices that are infected rather than providing remediation to all devices—including those that run on a different operating system that do not benefit from the remediation. *Id.*

The '697 patent provides further details on how to identify a computer's operating system, including a method that uses “TCP/IP stack fingerprinting to identify candidate operating systems based on the first SYN packet of the TCP

session” (*id.*, 3:50-53; *see also id.*, 6:51-7:7), as well as a different technique that is based on “User-Agent field on HTTP requests.” *Id.*, 3:53-55; *see also id.*, 7:9-13. The two techniques can also be combined to more accurately identify the operating system. *Id.*, 3:55-56.

In the network-based malware detection and remediation system described in Figure 1 of the '697 patent, an “edge node 112 either provides or is connected to one or more network sensors 130” that is capable of “copying packets of information traveling over the service provider SP network 110.” *Id.*, 4:50-54, Fig. 1.

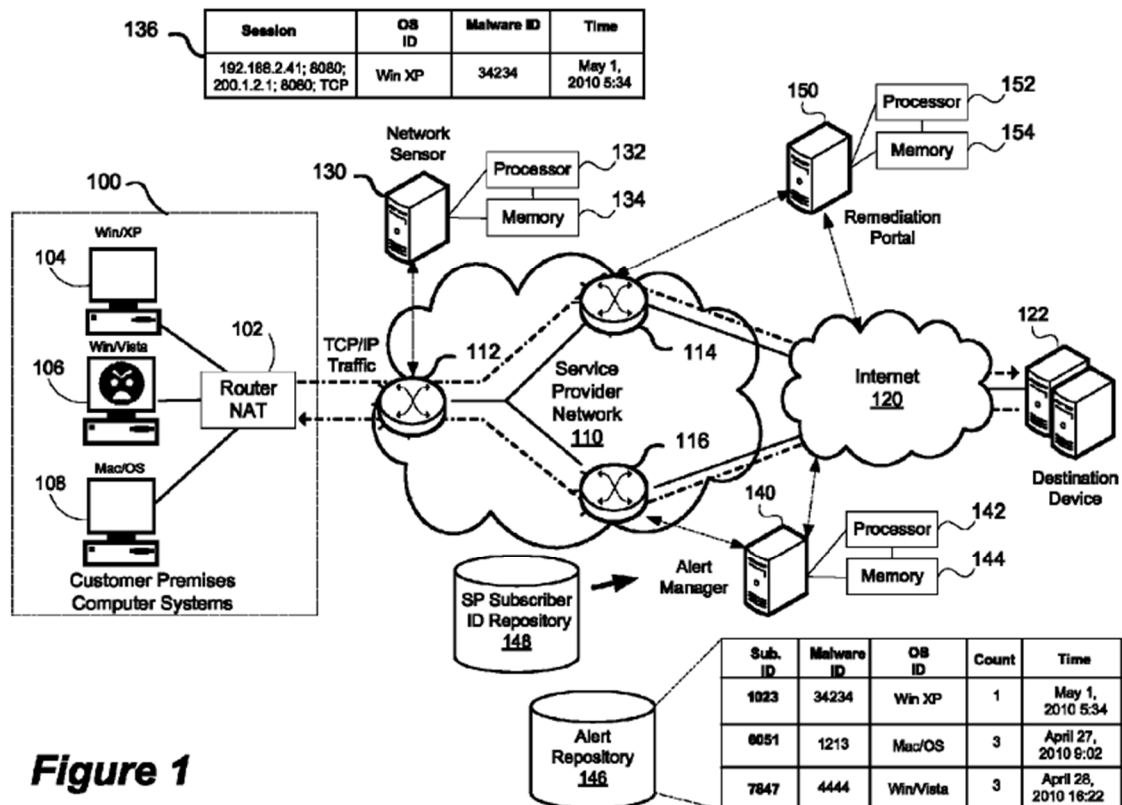


**Figure 1**

The network sensor 130 analyzes network packets, e.g., by comparing the packet data to malware signatures, to find evidence of possible malware. *Id.*, 4:55-58, 7:14-15. The network sensor 130 also examines the network “packets to determine the operating system (OS) of the computer 104 from which the packets originate.” *Id.*, 4:58-60.

“When the malware is identified, the network sensor 130 sends an alert 136 to an alert manager 140 coupled to the SP network 110 either directly or indirectly. The alert 136 contains ... [*inter alia*] the OS identifier of the computer that caused the alert, an identifier that indicates which specific malware was detected.” *Id.*, 4:60-5:2. The alert manager 140 also produces a subscriber notification including directions for accessing a remediation portal 150. *Id.*, 5:42-6:5. In this way, the remediation portal 150 can “determine the subscriber connecting to the portal and the operating system associated with the connection ... [and] then provide the subscriber with instructions to follow in order to remove or quarantine the particular malware detected if the OS matches the OS identified in the alert information 136.” *Id.*, 6:14-25.

Figures 4 through 8 of the '697 patent illustrate further details regarding operating system identification, malware detection and remediation (Figures 4 to 6), malware alert management (Fig. 7), and malware remediation (Fig. 8). *Id.*, 2:60-67.

**B. Independent Claims of the '697 Patent**

The '697 patent includes 25 claims, three of which—claims 1, 15 and 24—are independent claims. *Id.*, 10:30-13:15. Representative claim 1 is reproduced below, including the labels added by Petitioner to identify individual limitations.

**1[pre]:** A method of network based malware detection in a service provider network, the method comprising:

**1[a]:** receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;

**1[b]:** determining an operating system identifier (OS ID) associated with the TCP session and the computing device;

**1[c]:** determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and

**1[d]:** generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.

*Id.*, 10:30-45; Petition, ii.

Independent claim 15 is directed to a system and independent claim 24 is directed to a computer readable medium, and both claims include limitations that are

similar to claim 1, while claim 15 further recites “a plurality of network sensors.”  
Ex. 1001, 11:52-12:4, 12:53-13:3.

### **III. LEVEL OF ORDINARY SKILL IN THE ART**

Petitioner contends that “[a] POSITA, as of March 2011, would have been an individual with either (1) at least a bachelor’s degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer networking or security, or (2) at least 3 years of experience working on computer networking or computer security, even without a formal degree. EX1003, ¶16.” Petition, 10-11.

For the purposes of this Preliminary Response, Patent Owner relies on the definition proposed by Petitioner because Petitioner has not shown that any challenged claim is unpatentable even under this level of skill.

### **IV. CLAIM CONSTRUCTION**

Petitioner contends that all claims should be interpreted under their plain and ordinary meaning, and no claim term needs a specific construction.<sup>1</sup> Petition, 11.

---

<sup>1</sup> While the Petition acknowledges that no claim construction is needed,

Petitioner’s contradictory position in the parallel District Court Litigation purports

For the purposes of this Preliminary Response, Patent Owner agrees that no specific claim constructions are needed.

## **V. OVERVIEW OF REFERENCES USED IN THE PETITION**

Petitioner relies on the combination of three references—Deridder, Tuvell and Lee—in a single invalidity ground to assert that the Challenged Claims are invalid.

### **A. Overview of Deridder**

Deridder (Ex. 1006) is a U.S. Patent Application Publication No. 2010/0161795 A1, which shares an inventor, Darren Deridder, with the '697 patent. Ex. 1006, front page. Deridder was filed on December 22, 2009, claiming priority to a provisional application filed on December 22, 2008, and was published on June 24, 2010. *Id.* This reference relates to “methods and devices for identifying and tracking multiple computer user sessions associated with a network address translation (NAT) device coupled to a computer network.” *Id.*, Abstract.

In Figure 1, Deridder illustrates “a schematic representation of a system providing multi-user NAT session identification and tracking in a typical operating environment.” *Id.*, ¶10; Fig. 1. A traffic inspection device 150 can receive and

---

that 17 claim terms are indefinite. *See* IPR2026-00031, Paper 6, 6-9; Ex. 2005, 67-68.

inspect network traffic on the service provider network 110, which includes “routing devices, such as 112, 114 and 116 connected to additional networks such as the public internet 120 which external servers 122 are connected to.” *Id.*, ¶21. The system described in Deridder provides session tracking that allows “the sessions associated with multiple users (104 to 108) behind a NAT device 102 [] be detected, and their traffic [] be differentiated.” *Id.*

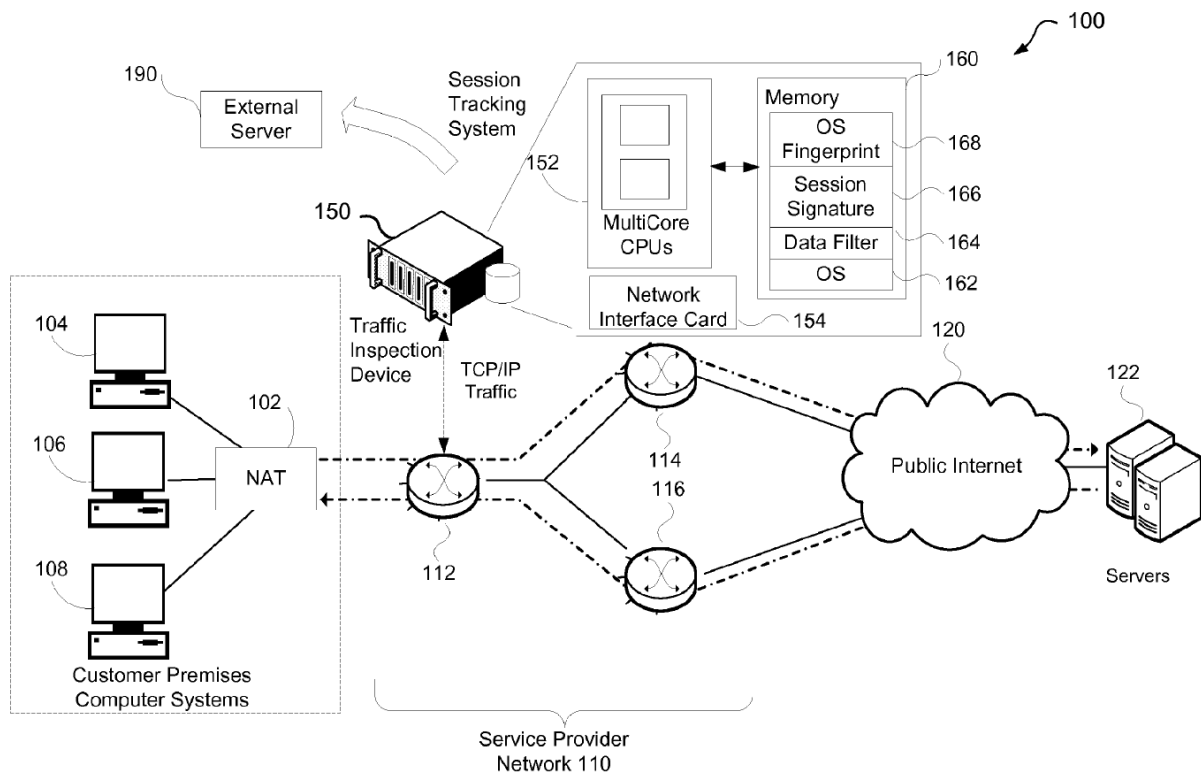


Figure 1

While Figure 1 of Deridder includes some components that are similar to some components in Figure 1 of the '697 patent, such as user devices (102, 104, 106) positioned behind a router/NAT 102 that communicates with a service provider

network 110, the Deridder reference has significant differences with the invention of the '697 patent. Ex. 2010, ¶¶48-49. Notably, Deridder has no description or details about malware, malware detection, malware remediation or equivalent, other than a single instance where malware detection is mentioned in the context of a “network interface card 154” in paragraph [0022]:

A network interface card 154 provides an interface to the Service Provider Network 110 for receiving packets for processing and enables communication with external servers 190 which provide services for utilizing the session tracking functionality for services such as network monitoring, targeted advertising, *malware detection*.

Ex. 1006, ¶22 (emphasis added); *see also* Ex. 2010, ¶¶48-49.

## **B. Overview of Tuvell**

Tuvell (Ex. 1004) is a U.S. Patent Application Publication No. 2008/0086773 A1, was filed on October 9, 2007, claiming priority to two provisional applications filed on October 6, 2006, and was published on April 10, 2008. Ex. 1004, front page. This reference relates to “a network management system [that] monitors malware within a mobile network.” *Id.*, Abstract.

Figure 3 of Tuvell provides further details of how Tuvell's network management system 100 (also referred to by Tuvell as CoreStats) is deployed. *Id.*, ¶¶15, 25. The network management system 100 includes “a receiver component 102

that obtains or receives malware data for a mobile network.” *Id.*, ¶25. The analysis component 104 “receives information from the receiver component 102 regarding the presence, effects and types of malware impacting a mobile network. In an embodiment, the analysis component 104 is able to synthesize malware data received from the plurality of sources to better analyze the nature and effect of malware. In another embodiment, the analysis component 104 generates a malware analysis or report that details and describes instances of malware in the mobile network and the particular mobile devices affected by malware.” *Id.*, ¶27.

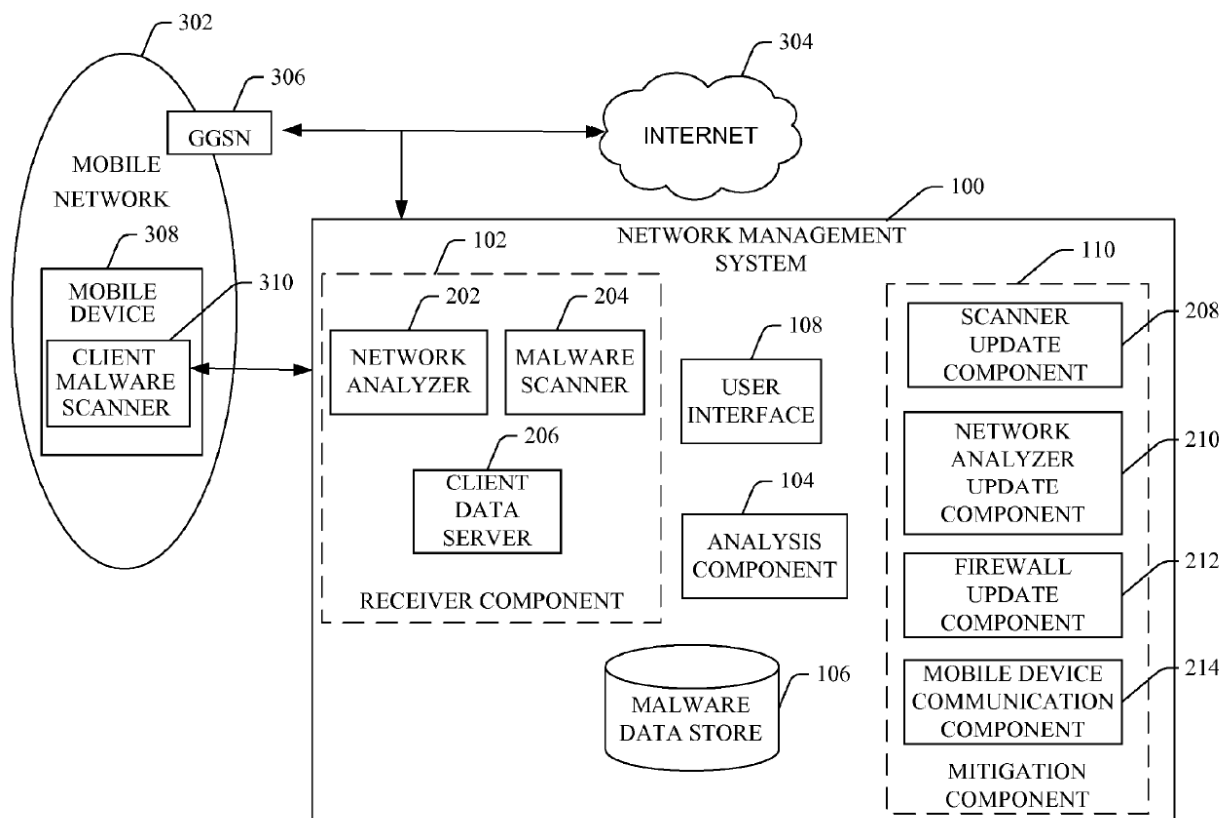


**FIG. 3**

In certain embodiments, a client data server receives reports of viruses or other malware from one or more client mobile devices. *Id.*, ¶35. “Individual mobile devices utilize scanning software to determine when malware is present and transmit malware or infection reports to the mobile network.” *Id.* Tuvell also explains that such “malware reports include device specific information such as current device hardware, software and/or an identifier for the infected mobile device (e.g., telephone number).” *Id.* “In certain embodiments, malware data obtained by the network analyzer 202 and client data server 206 includes device-specific information. In particular, reports received by the client data server 206 include data identifying the particular device that detected the malware... Such device specific information is critical in analysis and reaction to the presence of malware within a network.” *Id.*, ¶36.

The teachings in Tuvell are clearly different from the claimed invention in the '697 patent, in which the claimed operations are executed entirely on the service provider network side to provide alerts. *See, e.g.*, Ex. 1001, 10:30-45. These alerts can enable operators at a user location, on the other side of a NAT device, to provide more efficient remediation. Tuvell's technique, on the other hand, has components that are operating on both sides of NAT that “include a client malware scanner 310 capable of detecting malware on mobile client devices 308.” Ex. 1004, ¶45; *see also*

*id.*, ¶¶48-49. Tuvell represents a very different system compared to the invention in the '697 patent, and it has a different purpose. Ex. 1003, ¶¶51-53.

### **C. Overview of Lee**

Lee (Ex. 1005) is a Korean patent, which was published on April 26, 2006. Ex. 1005, 14. Based on the English translation of Lee provided by Petitioner,<sup>2</sup> this reference describes a system that analyzes network packets to determine conformity with security policy and presence/absence of intrusion, and relies on a virtual in-line network security module. *Id.*, Abstract.

The focus of Lee's invention appears to be in providing a "virtual in-line" module to inspect the traffic from a device or network as opposed to installing a "physical in-line" module that is physically placed in-line within the data path. *Id.*, ¶¶13, 26. The virtual in-line configuration is illustrated in Figure 2 of Lee, where the placement of components 16, 26 and 35 (annotated with red circles below; *id.*, ¶35, Fig. 2) are contrasted with Figure 1's physical in-line security equipment 15, 25 and 31 (annotated with red circles below). *Id.*, ¶¶22-23, Fig. 1. According to Lee, physical in-line network security equipment can slow down traffic and equipment failure can lead to network disconnection. *See e.g., id.*, ¶¶19, 24. In the

---

<sup>2</sup> The translation quality of Lee is quite poor, and it is often difficult to follow what it describes.

virtual in-line network security method, different in-line functions are mapped onto different processes that operate on network packets in sequence. *Id.* ¶30.

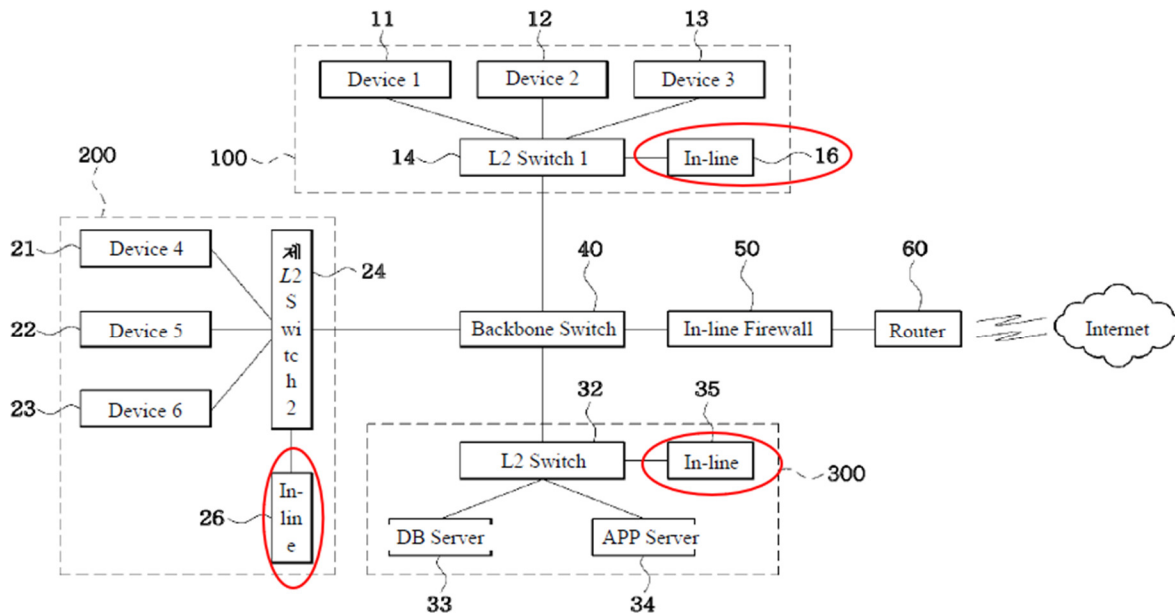


Figure 2 of Lee (annotated by Patent Owner)

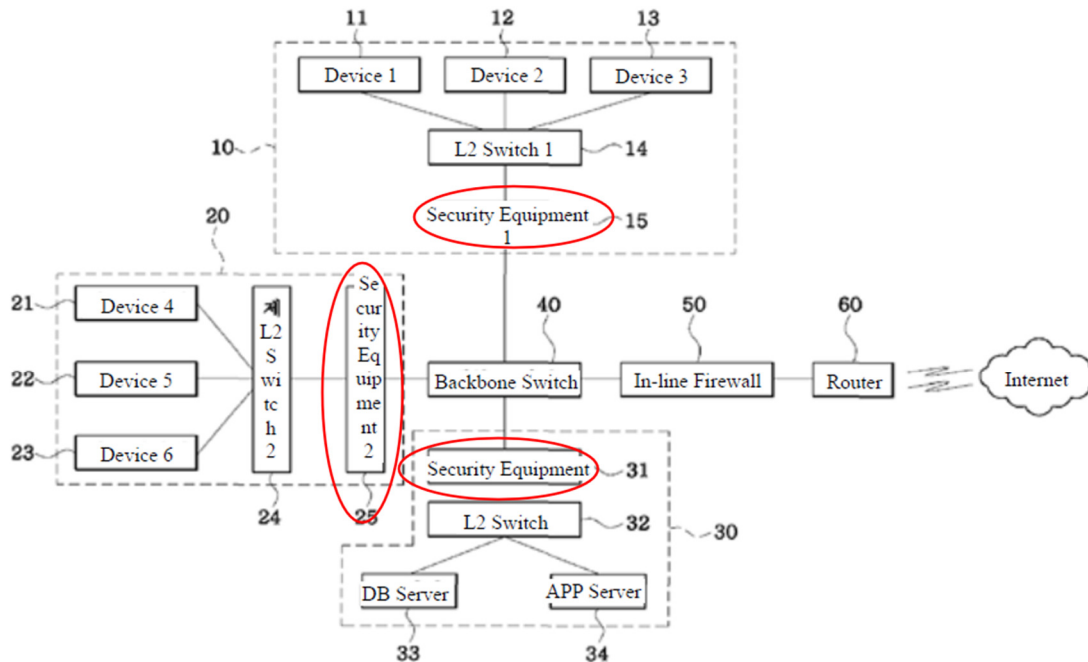


Figure 1 of Lee (annotated by Patent Owner)

Lee further provides a very short description related to Figure 5, where step 140 consists of “estimating (Guessing) the operating system (OS) of the extracted node,” followed by a Table where the OS is listed. *Id.*, ¶¶48-55, Fig. 5.

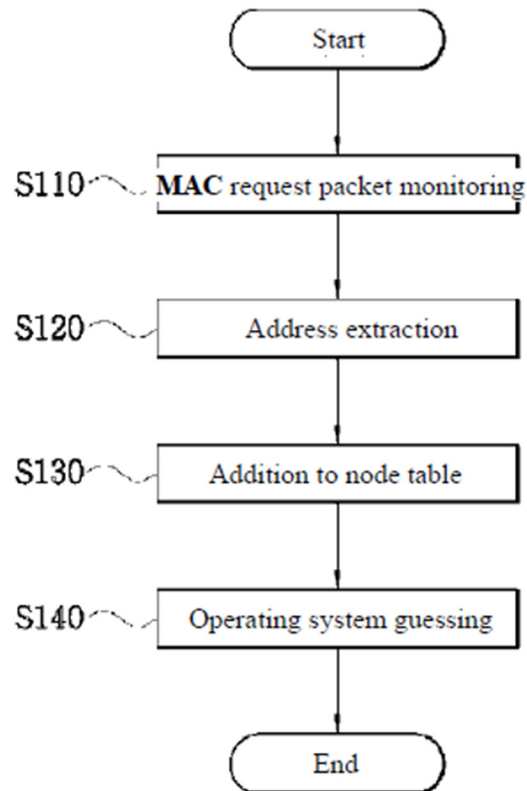


**Figure 5 of Lee**

[Node Table]

| MAC address       | IP address  | OS         | User  | Time    | Operation method |
|-------------------|-------------|------------|-------|---------|------------------|
| 00:13:D4:04:BD:C0 | 192.168.1.2 | Linux      |       |         | Allow            |
| 00:0F:EA:6D:71:2A | 192.168.1.1 | Windows XP | Kimpd |         | Virtual path     |
| 00:90:FB:09:0F:17 | 192.168.1.3 | Windows XP |       | ANYTIME | Separation       |

Aside from the above, Lee provides no other details about how the operating system is guessed, but explains that the OS information, along with the origin address, MAC address and other system conditions, are used to determine whether a system is “subject to a virtual path.” *Id.*, ¶41. This use of the OS information is irrelevant to the claimed invention of the '697 patent. *See* Ex. 2010, ¶¶54-55.

## **VI. THE PETITION FAILS TO SHOW THE CHALLENGED CLAIMS ARE UNPATENTABLE**

The Petition relies on the combination of Deridder, Tuvell and Lee to assert that claims 1-25 are obvious. As the following analysis shows, Petitioner's contentions are seriously flawed. Not only has Petitioner failed to show a proper motivation to combine, Petitioner also has not shown that individual claim limitations are rendered obvious by any one, or any combination, of Deridder, Tuvell and Lee.

### **A. A POSITA Would Not Have Found it Obvious to Combine Deridder with Tuvell and Lee**

As explained above in connection with overview of the Petition's references (*see* §V), Deridder, Tuvell and Lee each address a different problem and propose a different solution. These problems and solutions are different from one another, and are different from the claimed invention of the '697 patent. **Deridder** is about tracking network sessions and has no explanations about conducting malware

detection other than a passing reference to a network card (hardware component) that provides an interface with other devices. **Tuvell** describes a mobile network that relies on malware detection conducted by each individual device inside the mobile network; the report provided by individual mobile devices provide specific details about the infected device, including the device's phone number and OS information, all provided in the malware reports generated by the mobile devices themselves. **Lee** describes a system where instead of performing a physical in-line inspection of data traffic, virtual in-line components are used; its non-enabling description states that the operating system is "guessed" and used, in conjunction with other device-specific information, such as the device's MAC Address, IP Address and others, to determine which device should be "subject to a virtual path."

None of these references describe the claimed invention that relates to network based malware detection in a service provider network, with specific operations (e.g., elements 1[a] to 1[d] in claim 1) performed on the network side of the communication network to determine, *inter alia*, an operating system identifier based on TCP packets received at an access device, and to provide an alert with OS-specific information.

As Patent Owner's expert explains, a POSITA would be very unlikely to even consider these references next to each other, and would not know how to combine them to arrive at the claimed invention. Ex. 2010, ¶¶56-61.

Notably, Tuvell combines client-side information (information provided by individual mobile devices within the mobile network) with information on the network management system. Tuvell specifically discusses its reliance on the client-side malware scanner 310 (*see* Figure 3 annotated below) that detects malware on each mobile client device 308 inside the mobile network 302, and if malware is detected, the client-side malware scanner 310 generates an infection report 404 that provides malware data to the receiver component 102 on the network side. Ex. 1004, ¶¶35, 45, 48.

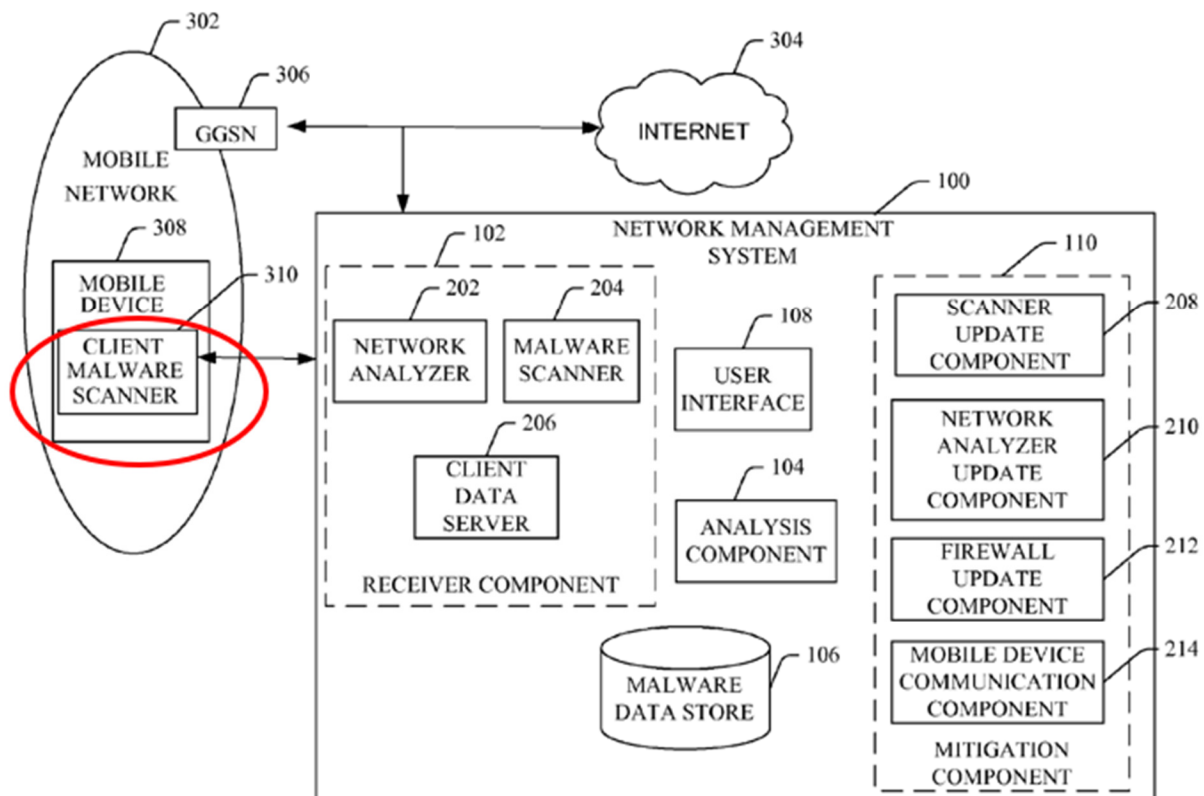


**FIG. 3**

Tuvell's reports generated by its client malware scanner 310 provide very specific and detailed information about the infected mobile device and "can include mobile device 308 information, such as the identification of the mobile phone (e.g., phone number), firmware of the particular mobile device 308 (e.g., operating system information) and the software version of the mobile device 308." Ex. 1004, ¶49. A POSITA reading Tuvell would have understood that Tuvell's teachings are do not describe the claimed invention of the '697 patent, where malware scanning and malware detection are performed on the service provider side; in the '697 patent the network traffic at the access device (e.g., NAT/gateway) is examined, where individual computing devices are connected to and are behind the access device (e.g., NAT/gateway) and cannot be distinguished. Ex. 2010, ¶¶57-58.

More importantly, a POSITA would have clearly understood that in Tuvell's system, the malware reports provided by the individual mobile devices already included all pertinent device-related information, down to a specific phone number and the OS information, and thus there would not be any need for network-side OS determination. Given that the mobile device in Tuvell had already provided its identify and its OS information, there would have been no reduction in the remediation effort on the user side of the NAT gateway once malware is detected. Notably, a POSITA would have recognized that Tuvell is a stand-alone solution and would have had no reason, and no reasonable expectation of success, to dismantle

Tuvell's technique by ignoring the user-side reports which was an integral part of Tuvell's malware detection. Ex. 2010, ¶¶57-58.

Additionally, as explained in connection with the overview of Deridder, this reference only includes a single reference to "malware detection" in the context of discussing an interface card, and provides no other details whatsoever. Given this dearth of explanations in Deridder, a POSITA in possession of both Deridder and Tuvell, even if contemplating to combine the two references, would have implemented the entire malware detection and scanning solution of Tuvell in Deridder, rather than cannibalizing Tuvell's technique and selectively picking and choosing certain elements of Tuvell in attempting to fit the '697 patent's features in hindsight. Tuvell's malware detection/remediation technique is significantly different from the claims of the '697 patent in several aspects, including its reliance on client-side malware scanning and already having precise information about each individual device that may have been infected. As Dr. Franz explains, "any attempt by Petitioner to propose a contrived combination would have been a far-fetched and unreasonable combination and it would not have even rendered the claims of the '697 patent obvious." Ex. 2010, ¶59.

Furthermore, Petitioner's use of Lee in the combination would not have made any sense to a POSITA. Petitioner uses Lee only for its explanation about estimating or guessing the Operating System information. Petition, 25-27, 29. But Lee does

not provide any explanations as to how OS information is guessed (or estimated), as admitted by Petitioner (*id.*, 28), and Lee's OS information (in conjunction with a number of other device parameters) is only used to determine which device would be subject to a virtual path. Ex. 1005, ¶¶41. Nothing in Lee provides any motivation to combine these teachings with Deridder and Tuvell, given that the selection of a virtual path is unrelated to any aspects of Deridder or Tuvell. Ex. 2010, ¶¶¶60-61.

Petitioner further purports that one reason for the combination (and it is unclear which of the references are being discussed) is to provide a cross-check in determining the OS ID, by using both fingerprinting and user-agent cross check. Petition, 19. While there are no requirements for a cross-check in the challenged independent claims, the only place where such a cross-check is discussed is in the '697 patent, where two different methods for determining OS information are combined to improve the accuracy of identification. Ex. 1001, 3:48-56; 8:50-9:20, Fig. 6. Critically, none of the references describe such a cross-check, and Petitioner's arguments are purely informed by the description in the '697 patent.

For at least the above reasons, Petitioner has failed to establish that a POSITA would have found it obvious to combine Deridder with Tuvell and Lee.

**B. The Combination Does Not Teach or Suggest 1[b]'s “*Determining an Operating System Identifier (OS ID) Associated with the TCP Session and the Computing Device*”**

Petitioner purports that the combination of Deridder and Tuvell renders element 1[b] (and similar elements in independent claims 15 and 24) obvious. Petition, 25-28. Petitioner argues that Deridder describes generating an OS fingerprint based on Deridder's explanation in paragraph [0031] that mentions a passive fingerprinting tool called “p0f.” *Id.*, 25-26, Ex. 1003, ¶98. But paragraph [0031] of Deridder includes additional explanations that are reproduced below:

However, unlike p0f, *the present system does not try to match the fingerprint to a list of known OS fingerprints*, because it is concerned less with the characterization of computer systems and more with the detection and tracking of unique sessions.

Ex. 1006, ¶31 (emphasis added).

The above section of Deridder clearly articulates that Deridder does not use the p0f tool to determine a specific OS, which contradicts element 1[b]'s requirement for determining an OS ID. Given the explicit instructions provided by Deridder, a POSITA would not have been motivated to ignore Deridder, and act in direct opposition to Deridder's guidance that “matching the fingerprint to a list of known OS fingerprints” is not necessary. Ex. 2010, ¶¶62-63. Furthermore, given

the different objectives of Deridder and the '697 patent as explained earlier in Section V, a POSITA would not have had any reason to perform an operation that expressly contradicts the description in Deridder by determining specific operating system information from the TCP session traffic or to enable OS-specific malware remediation for user devices that are behind the access device (e.g., NAT) of Deridder. *Id.*

Additionally, in Petitioner's narrative, a POSITA would start with Deridder and would supposedly find it obvious not only "to add malware detection to the service provider's network" but also to "use the OS fingerprinting in Deridder based on Deridder's explicit recognition of this." Petition, 17, 27; Ex. 1003, ¶¶85-86, 98. But, as explained earlier, Deridder only mentions malware detection in passing when describing a "network connection card." Ex. 1006, ¶22. There is nothing in that single recitation of "network connection card" or elsewhere in Deridder that would motivate a POSITA to provide specific malware detection operations that include using an operating system ID in a malware alert with the objective of reducing the workload of malware remediation. Such a hypothetical combination would have been far-fetched and not obvious. Ex. 2010, ¶64.

The Petition also appears to use Lee as part of its contention that element 1[b] is obvious. Petition, 28; Ex. 1003, ¶98. But Petitioner itself admits that Lee fails to explain how the OS information is obtained (Petition, 28), and Lee's use of

the OS information pertains to determining whether a system is “subject to a virtual path.” Ex. 1005, ¶41. Nothing in Lee’s description motivates or informs a POSITA to combine the OS identification of Lee with Deridder and/or Tuvell to perform element 1[b]. Ex. 2010, ¶65. In fact, because Tuvell’s system relied on client-side malware detection (within the mobile network by each mobile device), device-specific characteristics including the OS information and device-specific identity would have been known. This information included not only “type of mobile device 308, operating system, software and versions, and user information and mobile device 308 identifier,” but also “product identification that identifies the client malware scanner 310 software... and the mobile ... phone number.” Ex. 1004, ¶49. Therefore, there would have been no motivation to combine Tuvell with Lee, given that Tuvell’s client-side reports already provided such a comprehensive list of information, including the device’s operating system information. Ex. 2010, ¶66.

**C. The Combination Does Not Teach or Suggest Element 1[c]’s  
“*Determining If Malware Is Present in the TCP Session and an  
Associated Malware ID by Comparing a Malware Signature to the  
One Or More TCP Packets*”**

The Petition relies on Deridder to assert that the limitation in element 1[c] (and similar elements in independent claims 15 and 24) are obvious. Petition, 28-29, Ex. 1003, ¶99. Petitioner specifically points to Tuvell’s description of “malware signature searches [and] hash signature searches” in paragraph [0035] of Tuvell. Ex.

1004, ¶35; Petition, 28. Petitioner's position is flawed for several reasons. Ex. 2010, ¶¶67-70.

Unlike element 1[c] where a malware signature is compared to “one or more TCP packets,” paragraph [0035] of Tuvell describes performing a signature search or hash search of the software executing on the client mobile devices.

In a further embodiment, the receiver component 102 includes a client data server 206 *that receives reports of viruses or other malware from one or more client mobile devices. Individual mobile devices utilize scanning software to determine when malware is present and transmit malware or infection reports to the mobile network.* Some representative *malware scanning algorithms* for mobile devices include, but are not limited to, *malware signature searches; hash signature searches* as described in U.S. patent application Ser. No. 11/697,647 “Malware Detection System and Method for Mobile Platforms”; malware detection in headers and compressed parts of mobile messages as described in U.S. patent application Ser. No. 11/697,658 “Malware Detection System and Method for Compressed Data on Mobile Platforms ....

Ex. 1004, ¶35 (emphasis added).

The underlined sections of Tuvell's paragraph [0035] make clear that individual mobile devices utilize scanning software to determine if malware is present. Thus, any signature or hash searches to determine the malware is carried out by the individual mobile devices, and then malware reports are sent out to the network side. This contradicts element 1[c]'s requirement for network side "determining if malware is Present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets." Ex. 2010, ¶67.

Further, a POSITA would have been informed by the examples provided in paragraph [0035] of Tuvell, and would have understood that device-based "malware scanning algorithms" for mobile devices at the time of Tuvell primarily focused on examining the executable code on the mobile device to detect malicious programs. In this regard, Tuvell itself when referring to "hash signature searches" cites to U.S. patent application Ser. No 11/697,647 "Malware Detection System and Method for Mobile Platforms." See Ex. 1004, ¶35. This patent application issued as U.S. Patent No. 9,104,871 (Ex. 2011) and does not describe scanning TCP packets, but relates to scanning the software present on the mobile device to prevent the execution of malware that may already have been introduced to the device. *Id.*, Abstract, 5:63-6:55. Another patent document referred to in Tuvell's paragraph [0035] is U.S. patent application Ser. No 11/697,658 ("Malware Detection System and Method for

Compressed Data on Mobile Platforms) which issued as U.S. Patent No. 9,009,818 (Ex. 2012), describes a system for searching compressed and fragments mobile data (i.e., associated with mobile applications that are to be installed on mobile platforms) to discover specific search strings that correspond to byte sequences in known malicious executables. *Id.*, Abstract, 5:63-6:11.

The express teachings provided by Tuvell, supported by the references that Tuvell relies on, all describe signature and hash searches that are carried out by mobile devices, on the code or applications that reside on those mobile devices. This is in stark contrast to element 1[c] and claim 1 that is directed to a “method of network based malware detection in a service provider network” and all the elements of claim 1, including “determining if malware is present [...] by comparing a malware signature to the one or more TCP packets” are performed on the provider network side. Therefore, Tuvell fails to teach or suggest element 1[c] and claim 1 of the '697 patent. Ex. 2010, ¶¶68-70.

**D. The Combination Does Not Teach or Suggest Element 1[d]'s  
“Generating an Alert Identifying a Network Address Associated with  
the Access Device, the Malware ID and the OS ID Associated with  
TCP Session That Generated the Alert”**

Deridder, Tuvell or Lee fail to describe generating the specific alert that is recited in element 1[d] (and similar elements in claims 15 and 24). The Petition's position regarding obviousness of element [1d] appears to primarily rely on filling

the holes in the teachings of Deridder, Tuvell and Lee by purporting that this claim limitation would have been obvious to a POSITA. Petition, 29-30, Ex. 1003, ¶100.

Petitioner starts by asserting that Tuvell describes generating “a” report or alert. Petition, 29. But Tuvell’s purported report or alert does not include identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert, as recited in claim 1. Instead, Petitioner repeatedly invokes that inclusion of such specific information in the alert would have been obvious. *Id.*, 29-30. However, as explained earlier in Section VI.A, Petitioner has not shown that it would have been obvious to combine Deridder, Tuvell and Lee, let alone any hypothetical report that would be generated based on a combination of those disparate references.

Petitioner’s obviousness rationale is further flawed because Tuvell already described that each client-side mobile device provided a malware report and detailed information about each specific mobile device, including its operating system, the type of device, “software and versions,” user information, and indeed even “mobile device 308 information, such as the identification of the mobile phone (e.g., phone number)”. Ex. 1004, ¶49. In such a hypothetical combination, the client-side malware reports of Tuvell already provided detailed information identifying the client-side mobile device (including its OS) that were provided to the network side (CoreStats). *Id.*, ¶48. Petitioner’s combination requires generating the claimed

reports based on a fundamental architectural change in Tuvell's malware detection scheme and thus would not have been obvious to a POSITA. Ex. 2010, ¶¶71-73.

**E. The Combination Fails to Render Obvious Any of the Challenged Claims**

The Petition's obviousness assertions against independent claims 15 and 24 rely on the same flawed arguments as those used against claim 1 (Petition, 44-47) and therefore suffer from the same shortcomings as those discussed in connection with claim 1. Therefore, all independent claims of the '697 patent are patentable.

Because independent claims 1, 15 and 24 are patentable over the combination of Deridder, Tuvell and Lee, their dependent claims likewise remain patentable.

**VII. PETITIONER IMPROPERLY RELIES ON POSITA'S KNOWLEDGE INSTEAD OF DISCLOSURE OR TEACHING IN THE PRIOR ART REFERENCES**

On July 31, 2025, the Director's office issued a memorandum (the "July Memorandum") putting all practitioners on notice that the Office "will enforce and no longer waive the requirement of 37 C.F.R. § 42.104(b)(4) (Rule 104(b)(4)) that a petition for inter partes review (IPR) "must specify where each element of the claim is found in the prior art patents or printed publications relied upon"" and prohibiting reliance on "applicant admitted prior art (AAPA), expert testimony, common sense, and other evidence that is not "prior art consisting of patents or printed publications"

... to supply a missing claim limitation.” July Memorandum, 1. The July Memorandum makes clear that reliance on a “general knowledge,” such as by a POSITA, to fill in missing claim limitations from prior art reference(s) was impermissible and is limited to supporting motivation to combine and demonstrating the knowledge of a POSITA. *Id.*, 1-2. This change applies to any petition filed on or after September 1, 2025 (*id.*, 3) and, thus, applies to the instant Petition.

Petitioner disregarded the Director’s instructions. The Petition impermissibly relies on the knowledge of a POSITA to substitute for missing ’697 patent claim limitations in the combination of Deridder, Tuvell and Lee. The following highlights only a few instances.

**Element 1[b]:** The Petition admits the shortcomings of Lee, but impermissibly uses the knowledge of a POSITA to fill in the missing limitation:

Although Lee does not describe from where to extract the OS information, it would have been obvious to a POSITA that the User-Agent field in the HTTP header contains that information and could be easily extracted from there. EX1007, §§14.43, 3.8; EX1003, ¶98. A POSITA reviewing Lee would therefore have found it obvious to check the User-Agent field in the HTTP header to determine the OS. EX1003, ¶98.

Petition, 28. A review of ¶98 of Fortinet's expert declaration and Ex. 1007's cited sections<sup>3</sup> reveals no explanations about obtaining the OS information, but rather the mere statement that "[i]t is my opinion, that, in reviewing Lee, POSITA would have known to use the User-Agent field in the HTTP header to determine the OS." Ex. 1003 at ¶98. Notably, there is no explanation related to OS in the sections of Ex. 1007 cited by Petitioner and no explanations as to how the User Agent is used to determine the OS other than the statement that a POSITA would have known how to do so.

**Element 1[c]**: The Petition substitutes the knowledge of a POSITA to map comparison of the malware to a signature *to one or more TCP packets*:

Tuvell discloses determining if malware is present in the TCP session by using malware scanning algorithms, including "malware signature searches [and] hash signature searches." EX1004, ¶35. A POSITA would have understood that these searches involve comparing a malware signature to one or

---

<sup>3</sup> While Ex. 1007 and Petitioner's expert declaration fail to provide the missing limitation, Petitioner's reliance of arguments and evidence in the expert declaration amounts to improper incorporation by reference, which is prohibited under 37 C.F.R. § 42.6(a)(3).

more TCP packets to determine if malware is present.  
EX1003, ¶99.

Petition, 28. Examination of ¶99 reveals no explanations as to why or how Tuvell's malware signature searches involves comparison of the malware to a signature *to one or more TCP packets* other than the use of a POSITA's knowledge as a gap-filling measure: "I rely upon Tuvell to disclose and render obvious this limitation, *in combination with the knowledge of a POSITA.*" Ex. 1003, ¶99 (emphasis added).

**Element 1[d]**: The Petition relies on the knowledge of a POSITA for multiple missing aspects of element 1[d] which are not described in Tuvell:

Tuvell discloses that the analysis component 104 of the system "correlates data obtained from a variety of sources (e.g., network traffic, data network traffic and individual mobile devices 308)." EX1004, ¶54. *It would have been obvious to a POSITA that this correlation would have included the OS type determined by the OS fingerprinting technique in Deridder and the User-Agent field from Lee, since Tuvell already contemplated using other data to determine the OS type (OS ID).* EX1003, ¶100.

Petition at 29-30 (emphasis added). As evident from the above statement, Petitioner is stating that while Tuvell contemplated using other data to determine OS type, a

POSITA would have found it obvious to fill the gap that correlating the data in Tuvell would include producing the OS type (OS ID).

Petition's remaining explanations for element 1[d] is rife with substituting the knowledge of a POSITA for the missing elements involved in generating an alert in element 1[d]. Notably, Petition's explanation for element 1[d] starts on page 29, and *every sentence* after the first paragraph of this section (other than the sentence on p. 29 that starts with "For example" reproduced above), invokes the knowledge of a POSITA—7 times altogether. These flaws propagate throughout the Petition, including in Petitioner's invalidity assertions against independent claims 15 and 24.

This flaw in the Petition not only runs afoul of the July Memorandum and illustrates Petitioner's disregard for Rule 104(b)(4), but it also reveals significant shortcomings in the Petition's three-reference combination of Deridder, Tuvell and Lee that the Petitioner is now attempting to conceal by impermissibly relying on the knowledge of the POSITA. This provides a compelling reason for the Director to deny institution of the Petition.

## **VIII. CONCLUSION**

For the reasons discussed above, Patent Owner respectfully requests that the Director deny Petitioner's Petition for *Inter Partes* Review of the '697 patent.

Dated: January 14, 2026

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel

Babak Tehranchi, Reg. No. 55,937

Back-Up Counsel

Kyle Canavera, Reg. No. 72,167

Thomas Millikan, Reg. No. 72,316

Ashlee Sherman, (To be admitted – *Pro Hac Vice*)

*Attorneys for Netskope, Inc.*

PERKINS COIE LLP  
11452 El Camino Real, Ste. 300  
San Diego, CA 92130

**CERTIFICATE OF WORD COUNT UNDER 37 CFR § 42.24(d)**

Under 37 C.F.R. § 42.24(d), the undersigned certifies that the word count for this Patent Owner's Preliminary Response to the Petition for *inter partes* review totals 6,321 words, excluding the parts exempted by 37 C.F.R. § 42.24(a). The word count was made using the built-in word count function in the Microsoft® Word software used to prepare this document.

Dated: January 14, 2026

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel

Babak Tehranchi, Reg. No. 55,937

PERKINS COIE LLP  
11452 El Camino Real, Ste. 300  
San Diego, CA 92130

Back-Up Counsel

Kyle Canavera, Reg. No. 72,167

Thomas Millikan, Reg. No. 72,316

Ashlee Sherman, (To be admitted – *Pro Hac Vice*)

*Attorneys for Netskope, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 14<sup>th</sup> day of January 2026 true and correct copies of the foregoing NETSKOPE, INC.'S PRELIMINARY RESPONSE and EXHIBITS were served via electronic mail on Petitioner's counsel at the following address:

Andrew D. Gish (Reg. # 67,562)  
andrew@gishpllc.com  
Ryan Iwahashi (Reg. # 63,378)  
ryan@gishpllc.com

Dated: January 14, 2026

Respectfully submitted,

PERKINS COIE LLP  
1888 Century Park East, 17<sup>th</sup> Floor  
Los Angeles, CA 90067

/ Anita Chou /  
Anita Chou  
Patent Paralegal