IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

DECLARATION OF DR. ERIC COLE REGARDING CLAIM CONSTRUCTION

In re: Taasera Licensing, LLC Patent Litigation

Case No. 2:22-md-03042-JRG

July 13, 2023

TABLE OF CONTENTS

Page(s)

I. QUALIFICATIONS AND BACKGROUND INFORMATION

1. My name is Dr. Eric Cole. I am over eighteen years of age and I would be competent to testify as to the matters set forth herein if I am called upon to do so.

2. I have been retained by Fabricant LLP, counsel for the Plaintiff Taasera Licensing LLC (hereinafter referred to as "Taasera" or "Plaintiff"), in connection with this action to consider how one of ordinary skill in the art to which the Asserted Patents in this action are directed would have understood (at the time of the invention) the claim terms set forth in this Declaration. I may also be asked to rebut the proposed constructions and/or indefiniteness of the Asserted Patents that Defendants propose in their claim construction disclosures.

3. This Declaration contains my opinions with respect to the subject matter of this proceeding and with the understandings as set forth herein. I specifically reserve the right to formulate and offer additional or supplemental opinions based on any additional information, discovery, or evidence that may be provided or derived, future court rulings, or agreements between the parties, to the extent permitted by the Court.

4. For purposes of this Declaration, the Asserted Patents are: 6,842,796; 7,673,137; 8,327,441; 8,819,419; 8,850,517; 8,955,038; 8,990,948; 9,071,518; 9,092,616; 9,118,634; 9,608,997; 9,628,453; 9,860,251; and 9,923,918.

5. I anticipate being called to provide expert testimony before the U.S. District Court for the Eastern District of Texas regarding my opinions formed, resulting from my review of the Asserted Patents, the relevant file histories, the priority documents, the materials attached to this Declaration, my experience in the field of the inventions, and any invalidity arguments or contentions raised by Defendants. If called, I will so testify.

6. I am president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia.

7. I hold a master's degree in computer science and a doctorate in information security and have worked in the cyber and technical information security industry for over twenty-five years.

8. To briefly summarize, during my twenty-five-plus year security career I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; and 6) continually taught and written about cybersecurity.

9. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured.

10. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems.

11. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting client's information, helping them implement effective security solutions.

12. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people over live, online, and in person training sessions.

13. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

14. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

15. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a commissioner on cybersecurity for President Obama. My eight books on cybersecurity include "Cyber Crisis", "Online Danger," "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," "Insider Threat," and "Hackers Beware". which have become recognized as industry-standard sources. They are used in many classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

16. The focus of my work over the last ten years has been on data protection for commercial organizations. I am familiar with best practices in cybersecurity and have developed many of the standard practices. I am also very experienced both with the minimum required security necessary to protect client information, as well as the more enhanced measures considered best practices.

17. I am the founder of Secure Anchor Consulting, where I provide cybersecurity

consulting services and lead research and development initiatives to advance information systems security. Many of the clients I work with are responsible for protecting sensitive client and/or consumer information and implementing effective security.

18. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls and have detailed knowledge of the effort that is required to implement various remediation measures.

19. Today, my consulting efforts help organizations properly protect client information and various alternative methods of security that can be implemented. This includes hardening of systems, securing services, proper configuration, patching and compensating controls. I am familiar and experienced with proactive, cost-effective measures needed to protect client information; I ensure that organizations meet both contractual and policy requirements during this process.

20. I have a detailed understanding of balancing functionality with security. I am familiar and experienced with proactive, cost-effective measures needed to protect client information. I have worked to ensure that organizations meet both contractual and policy requirements in protecting client information.

21. I have led, and been involved in, responses to many cybersecurity incidents. This included performing root cause analysis, verifying the appropriateness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to

responding to breaches post detection. I have a detailed understanding of what is and is not an appropriate level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

23. Because of my background, training, and experience, I am qualified as an expert to opine on the issues with which I have been tasked. A more detailed account of my work experience and other qualifications is listed in my Curriculum Vitae attached as **Attachment A**. My CV also includes a list of my publications over the past ten years.

24. In forming my opinions, I rely on my knowledge and experience in the fields relevant to this Declaration. I further rely on documents and information referenced in this Declaration.

II. UNDERSTANDING OF THE APPLICABLE LAW

25. I understand that claim terms should be given their ordinary and customary meaning within the context of the patent in which the terms are used, *i.e.*, the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention in light of what the patent teaches, unless it appears that the inventors were using them to mean something else. Additionally, the specification and prosecution history must be consulted to confirm whether the patentee has acted as his/her own lexicographer (*i.e.*, provided special meaning to any disputed terms), or intentionally disclaimed, disavowed, or surrendered any claim scope).

26. I understand that a person of ordinary skill in the art is deemed to read a claim term not only in the context of the particular claim in which the disputed term appears, but also in the context of the entire patent, including the specification and the prosecution history. The prosecution file history provides evidence of how both the Patent Office and the inventors

understood the terms of the patent, particularly in light of what was known in the prior art. Further, where the specification describes a claim term broadly, arguments and amendments made during prosecution may require a more narrow interpretation. For these reasons, the words of the claim must be interpreted in view of, and be consistent with, the entire specification. The specification is the primary basis for construing the claims and provides a safeguard such that correct constructions closely align with the specification. Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim as set forth in the patent itself.

27. I understand that, to determine how a person of ordinary skill would understand a claim term, one should look to those sources available that show what a person of skill in the art would have understood disputed claim language to mean. Such sources include the words of the claims themselves, the remainder of the patent's specification, the prosecution history of the patent (all considered "intrinsic" evidence), and "extrinsic" evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art. I understand that one looks primarily to the intrinsic patent evidence, but extrinsic evidence may also be useful in interpreting patent claims when the intrinsic evidence itself is insufficient.

28. Additionally, the context in which a term is used in the Asserted Claim can be highly instructive. Likewise, other claims of the patent in question, both asserted and not asserted, can inform the meaning of a claim term. For example, because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

29. I understand that, while intrinsic evidence is of primary importance, extrinsic

evidence, *e.g.*, all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises, can also be considered. For example, technical dictionaries may help one better understand the underlying technology and the way in which one of skill in the art might use the claim terms. Extrinsic evidence should not be considered, however, divorced from the context of the intrinsic evidence. Evidence beyond the patent specification, prosecution history, and other claims in the patent should not be relied upon unless the claim language is ambiguous in light of these intrinsic sources. Furthermore, while extrinsic evidence can shed useful light on the relevant art, I understand that it is less significant than the intrinsic record in determining the legally operative meaning of claim language.

30. I understand that the Supreme Court of the United States has instructed that, in order for a claim to be definite, "a patent's claims, viewed in light of the specification and prosecution history, [must] inform those skilled in the art about the scope of the invention with reasonable certainty." The Supreme Court also warned that "the definiteness requirement must take into account the inherent limitations of language . . . Some modicum of uncertainty . . . is the price of ensuring the appropriate incentives for innovation." The Court also stated that "a patent must be precise enough to afford clear notice of what is claimed, thereby apprising the public of what is still open to them."

31. I understand that a patent claim may be expressed using functional language. 35 U.S.C. § 112 ¶ 6 provides that a structure may be claimed as a "means . . . for performing a specified function" and that an act may be claimed as a "step for performing a specified function." There is a rebuttable presumption that § 112 ¶ 6 applies when the claim language includes "means" or "step for" terms, and that it does not apply in the absence of those terms. The presumption stands or falls according to whether one of ordinary skill in the art would understand the claim

with the functional language, in the context of the entire specification, to denote sufficiently definite structure or acts for performing the function.

32. When it applies, § 112 ¶ 6 limits the scope of the functional term to only the structure, materials, or acts described in the specification as corresponding to the claimed function and equivalents thereof. Construing a means-plus-function limitation involves multiple steps. The first step is a determination of the claimed function of the means-plus function limitation. The next step is to determine the corresponding structure disclosed in the specification and equivalents thereof. A structure disclosed in the specification is "corresponding" structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim. The focus of the "corresponding structure" inquiry is not merely whether a structure is capable of performing the recited function, but rather whether the corresponding structure is clearly linked or associated with the recited function. The corresponding structure must include all structure that actually performs the recited function. However, § 112 ¶ 6 does not permit incorporation of structure from the written description beyond that necessary to perform the claimed function.

33. For § 112 ¶ 6 limitations implemented by a programmed general purpose computer or microprocessor, the corresponding structure described in the patent specification must include an algorithm for performing the function. The corresponding structure is not a general purpose computer but rather the special purpose computer programmed to perform the disclosed algorithm.

34. I understand that, in general, a term or phrase found in the introductory words of the claim, the preamble of the claim, should be construed as a limitation if it recites essential structure or steps, or is necessary to give life, meaning, and vitality to the claim. Conversely, a preamble term or phrase is not limiting where a patentee defines a structurally-complete invention

in the claim body and uses the preamble only to state a purpose or intended use for the invention. In making this distinction, one should review the entire patent to gain an understanding of what the inventors claimed they actually invented and intended to encompass by the claims.

35. I understand that language in the preamble limits claim scope: (i) if dependence on a preamble phrase for antecedent basis indicates a reliance on both the preamble and claim body to define the claimed invention; (ii) if reference to the preamble is necessary to understand limitations or terms in the claim body; or (iii) if the preamble recites additional structure or steps that the specification identifies as important. Otherwise, the preamble is not limiting.

36. It is also my understanding that method claims do not generally require the cited steps to take place in any particular order.

37. I also understand that a court may correct obvious minor typographical and clerical errors in patents. Correction is appropriate only if (1) the correction is not subject to reasonable debate based on consideration of the claim language and the specification; and (2) the prosecution history does not suggest a different interpretation of the claims. The error must be evident from the face of the patent, and the determination must be made from the point of view of one skilled in the art.

38. Other considerations I made, detailed below, help one to achieve a proper interpretation of the claims.

III. MATERIALS CONSIDERED

39. In forming my opinions, in addition to my knowledge and experience, I have considered the materials cited in and/or attached to this Declaration and the following documents which either I have obtained or have been provided to me:

- the Asserted Patents and their file histories;

- the priority documents for the Asserted Patents and their file histories;
- the parties' claim construction documents;
- the prior art documents referenced in any Invalidity Contentions; and
- the materials attached to this Declaration.

40. In addition to the materials provided to me, I have also relied on my own education, training, experience, and knowledge in the field of data communications, information storage management and distribution, including multimedia.

41. I may rely on any of these materials, experiences, and knowledge, in addition to the evidence specifically cited as supportive examples in particular sections of this Declaration, as additional support for my opinions.

42. I reserve the right to supplement or amend this Declaration if additional facts and information that affect my opinions become available.

IV. LEVEL OF ORDINARY SKILL IN THE ART

43. It is my understanding that I must address the issues set forth in this Declaration from the viewpoint of a person of ordinary skill in the art at the time of the invention to which the Asserted Patents pertain.

44. It is my opinion that the person of ordinary skill in the art ("POSITA") would have a bachelor's degree in electrical or computer engineering or computer science with two to four years of experience in the field of network security. Extensive experience and technical training might substitute for educational requirements, while advanced degrees, such as a relevant M.S. or Ph.D., might substitute for experience. I also understand that the Asserted Patents are entitled to the below priority dates, and that is the relevant time period from which a person of ordinary skill in the art would evaluate the disclosure of the Asserted Patents:

45. I understand that the Asserted Patents are entitled to the below priority dates, and that is the relevant time period from which a POSITA would evaluate the disclosure of the Asserted Patents:

- Each of the asserted claims of the '422 Patent is entitled to a priority date of February 17, 2011;
- Each of the asserted claims of the '038 Patent, the '997 Patent, and the '918 Patent is entitled to a priority date of December 21, 2005;
- Each of the asserted claims of the '518 Patent is entitled to a priority date of July 1, 2011; and
- Each of the asserted claims of the '948 Patent and the '616 Patent is entitled to a priority date of May 1, 2012;
- Each of the asserted claims of the '137 Patent is entitled to a priority date of January 4, 2002;
- Each of the asserted claims of the '441 Patent is entitled to a priority date of February 17, 2011;
- Each of the asserted claims of the '517 Patent is entitled to a priority date of January 15, 2013;
- Each of the asserted claims of the '796 Patent is entitled to a priority date of July 3, 2001;
- Each of the asserted claims of the '356 Patent is entitled to a priority date of August 27, 2003;
- Each of the asserted claims of the '419 Patent, the '634 Patent, the '453 Patent, and the'251 Patent is entitled to a priority date of April 3, 2003.

V. CLAIM CONSTRUCTION

A. "an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module" – '137 Patent Claim 1

46. I understand that Defendants contend that this term is subject to § 112 ¶ 6 and indefinite, while Plaintiff contends that this term is subject to § 112 ¶ 6 and not indefinite.

47. Since the parties do not dispute that the term is subject to § 112 ¶ 6, I do not express an opinion regarding the structure in the claim.

48. The parties also agree that the function that should be accorded to this term is "monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module."

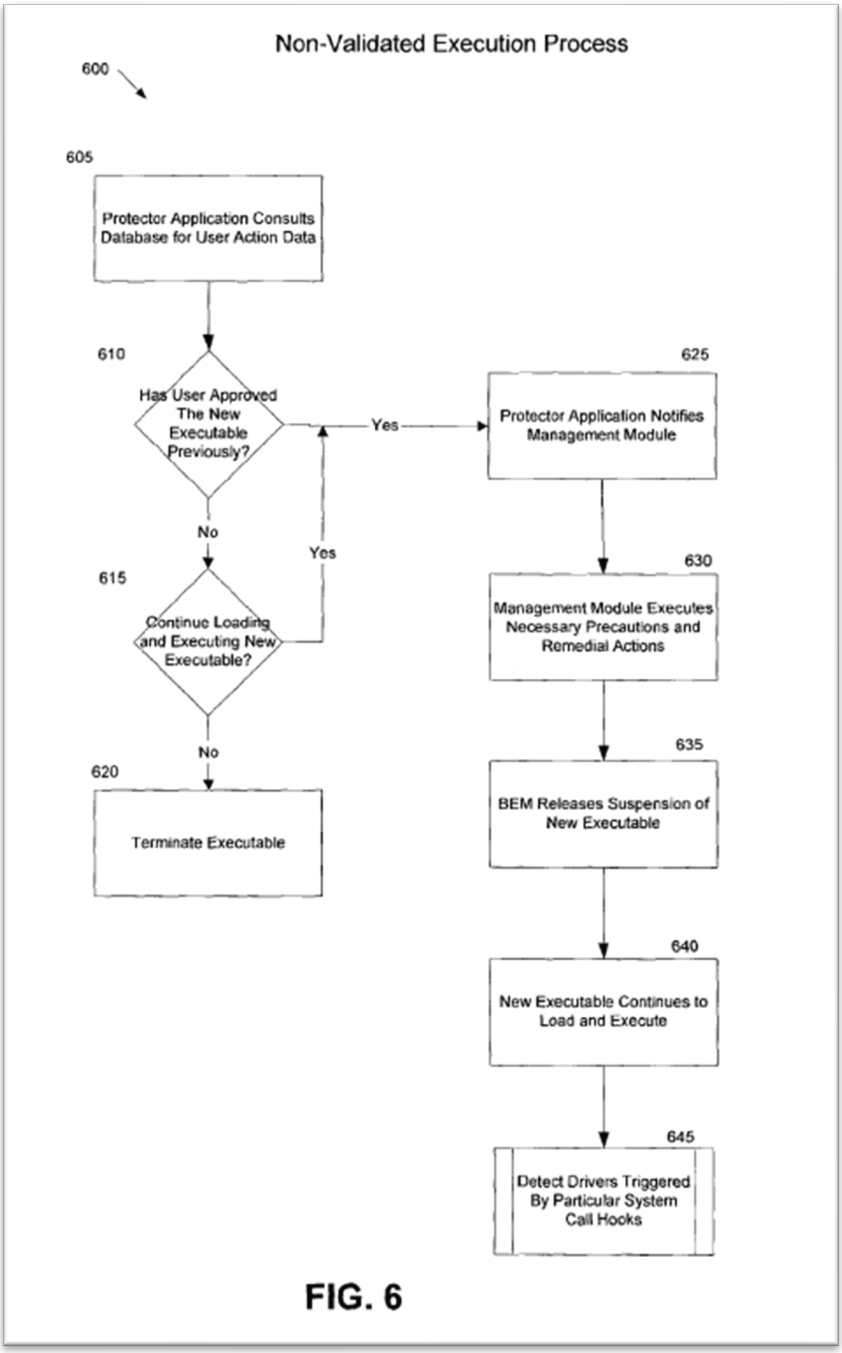
49. The parties dispute, however, the structure that should be accorded to this term. Defendants contend that the term is indefinite because the specification fails to disclose adequate structure, while the Plaintiff contends that the structure is the software algorithm performing the steps of Figure 6.

50. In my opinion, the POSITA would understand that Figure 6 and its supporting text are clearly linked to the "execution module," and that the steps of this algorithm should be construed to be the corresponding structure. The execution module monitors the program while it is executing, in contrast from the pre-execution module, which monitors the program before it is installed or executed. *See* '137 Patent, 3:20-4:18.

51. Figure 6, according to the patent, discloses "a logic flow diagram illustrating a non-validated execution process using the protector system in accordance with an exemplary embodiment of the present invention." *Id.* at 4:40-42. The algorithm in Figure 6 occurs "after the pre-execution process and concern[s] executable files that the binary execution monitor 125 could

not validate in the pre-execution phase. Referring to FIG. 6, an exemplary process 600 is illustrated for executing an executable file that has not been validated." *Id.* at 9:38-43.

52. Figure 6, shown below, explicitly discloses the steps performed by the "execution module" when a non-validated program is running:



Id. at Fig. 6.

53. In my opinion, the execution module is explicitly referring to the ***non-validated execution process*** of Fig. 6, which is implemented through the structure of a software algorithm. One of the benefits of the claimed invention is performing a validation step during the pre-execution process to minimize the amount of unnecessary monitoring and false positives of security alarms during program execution. The purpose of the execution module is ***monitoring a non-validated program as the program is being executed***. Such a benefit and understanding is supported by the '137 patent and my own experience. *See id.* at 10:49-61 ("The pre-execution process provides an efficient method for determining whether an uncorrupted program is allowed to execute. By validating certain programs during the pre-execution process, the protector system minimizes the amount of work that must be done in monitoring and controlling programs during the execution phase. The validation step also reduces the number of false positive alarms, thereby reducing security interruptions for the user.")

B. "network administration traffic" – '356 Patent, Claims 1, 2, 9, 10, 13, 14, 17, and 18

54. I understand that Defendant contends that this term is indefinite, while Plaintiff contends that it should be construed to mean "traffic generated by harmless network administration activities."

55. The claims of the '356 patent are clear to the POSITA that network administration traffic is harmless traffic that is known to be benign or harmless, and therefore can be ignored by the security system:

> 1. A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:
>
> a computer-readable tangible storage device;
>
> first program instructions to determine if the packet is a known exploit;

> second program instructions to determine if the packet is addressed to a broadcast IP address of a network;
>
> ***third program instructions to determine if the packet is network administration traffic***;
>
> fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR ***the packet being network administration traffic, to determine that the packet is not a new, exploit candidate***; and
>
> fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND ***the packet not being network administration traffic*** AND ***the packet not being another type of traffic known to be benign***, to determine and report that the packet is a new, exploit candidate; and wherein
>
> the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device.

56. The specification also informs the POSITA as to the meaning of "network administration traffic" in the context of the '356 patent. For example, the summary of the invention section informs the POSITA that, if the packet is already a known exploit, or is network broadcast traffic, or is network administration traffic, then the packet is not considered a new exploit candidate. 3:11-20. Figure 7, copied below, also discloses a program function within the filtering algorithm that "determines if the current packet is harmless network administration traffic":

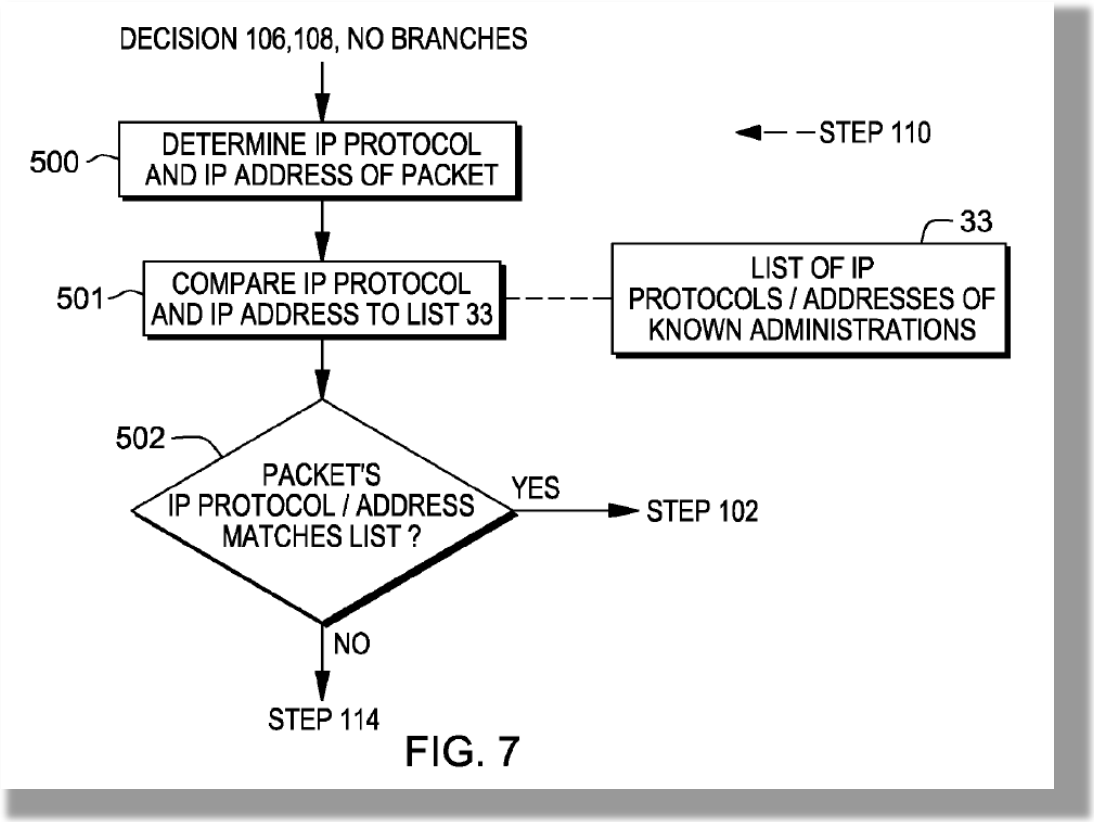


FIG. 7

57. In my opinion, the POSITA would understand the claims' use of "network administration traffic" to be "traffic generated by harmless network administration activities" as proposed by Plaintiff. For example, the specification discloses that network administration traffic is "presumed to be harmless":

> If the packet is network administration traffic, it is presumed to be harmless, and honeypot 12 proceeds to step 102 as described above.

'356 Patent, 5:59-60.

58. The specification also provides a non-limiting list of examples of network administration traffic that can be presumed to be harmless, including "secure shell ("SSH") traffic to remotely install a patch or change configuration or virtual network computing ("VNC") traffic or terminal services traffic to create a remote server desktop to remotely add a userID, or install a patch or change configuration (decision 110)." *Id.* at 5:54-59.

59. The POSITA would also understand that scanning and monitoring all routine traffic, including benign network administration traffic would be a waste of resources and computing power. Therefore, a benefit of the claimed invention is ignoring packets from presumptively harmless network administration traffic, which saves valuable resources and leads to a more efficient system. One of those valuable resources is time. For example, it is time consuming to parse every network packet for known attacks, where each packet must have a purpose or explanation before they are discounted as known or harmless. As the '356 patent explains (and is supported by my own experience), "the shear [sic] number of packets received by [such a] honeypot delays the detection of new computer attacks, viruses, computer worms and exploitation code." *Id.* at 2:38-3:5.

60. Because the claims and the specification routinely and consistently refer to network administration traffic as harmless network traffic, the benefit to streamlining analysis by classifying network administration traffic as benign, and specific examples of the types of network administration traffic, my opinion is that the POSITA would have understood this term to not be indefinite and to be accorded the construction "traffic generated by harmless network administration activities."

C. "[third/fourth] program instructions to determine if the packet is network administration traffic" – '356 Patent, Claims 1, 9, 10, 13, and 17

61. I understand that Plaintiff and Defendants agree that this term is subject to § 112 ¶ 6.

62. I also understand that Plaintiff and Defendants agree that the function that should be accorded to this term is "determine if the packet is network administration traffic."

63. I also understand that Plaintiff contends that the structure that should be accorded to this term is "Software algorithm that performs the steps of FIG. 7" while Defendants contain

that the term lacks sufficient structure and is therefore indefinite.

64. I agree with the Plaintiff and Defendant that the "program instructions" are subject to § 112 ¶ 6.

65. I agree with Plaintiff that the algorithm of Figure 7 is clearly linked to the determination of whether the packet is network administration traffic and, therefore, is the algorithmic structure that should be accorded to this term.

66. The specification of the '356 patent clearly and unambiguously links Figure 7 to the determination of whether the packet is network administration traffic:

> FIG. 7 is a flow chart illustrating a program function within the honeypot packet filtering program of FIG. 2 which determines if the current packet is harmless network administration traffic.

'356 Patent, 4:1-4.

> FIG. 7 illustrates in more detail decision 110 of FIG. 2 ***(i.e. determining if the current packet is network administration traffic presumed to be harmless***). Some or all bonafide network administrators are known to the administrator of intranet 14 by their combinations of IP protocol and respective IP address. These combinations were entered by the administrator and stored in a list 33 within honeypot 12. (Examples of the protocols used by a network administrator are SSH and Tellnet.) So, program 30 determines the IP protocol and IP address of the current packet by parsing the packet header (step 500). Then, program 30 compares the combination of IP protocol and IP address of the current packet to the combinations on the list 33 (step 501). If there is a match (decision 502, yes branch), then the current packet is deemed harmless network administration traffic, and program 30 proceeds to step 102 as described above. If there is no match, then program 30 proceeds to decision 114 as described above.

Id. at 8:21-37 (emphasis added).

67. It is my opinion that the POSITA would have understood this structure to be an algorithm with several steps. For example, the specification clearly teaches the POSITA that the

first step is to determine the IP protocol and IP address of the packet by parsing the header. *Id.* at 8:31-37. Then, the second step is to compare that information to a list. *Id.* Third, if there is a match between the header info and the list, the packet is deemed to be network administration traffic that is presumed to be harmless. *Id.*

68. Therefore, it is my opinion that "[third/fourth] program instructions to determine if the packet is network administration traffic" should be construed under § 112 ¶ 6 with the Structure, "Software algorithm that performs the steps of FIG. 7," and the Function, "determine if the packet is network administration traffic."

D. "determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request" – '419 Patent Claim 10

69. I understand that Defendants contend that this term is indefinite, and that Plaintiff contends it should be accorded its plain meaning.

70. A POSITA would understand this claim limitation from the claim language itself, the preceding claim limitations, and support of this plain claim language in the specification. A user (*e.g.*, through a browser) sends a resource request (*e.g.*, webpage request) to a computer, which has a network location. The resource requests contains a universal resource locator (URL).

71. Before transmitting the request, the computer evaluates whether any part of the URL needs to be encrypted. One example of such an evaluation is whether the URI portion of the requested URL was in plain text or encrypted in the first instance. *See* '419 Patent, 6:41-51. As the patent specification notes, the computer "determines whether the URL of the original resource request requires encryption prior to transmission of the request. The encryption analysis occurs after the determination of the destination location of the message so as to not misdirect the message during transmission. If the URL requires encryption, step 43 encrypts the URL…The encryption of the URL could be a partial encryption or a total encryption." *Id.*, at 6:10-31. After transmission,

the computer determines whether the requested resource is available, and uses the encrypted URL to locate the requested resource. What follows in the process is the claim limitation in question that provides the requested resource to the user (*e.g.*, via a web browser) with its accompanying URL that may or may not be encrypted.

> If the resource is to be returned without a URL change, then the process moved to step 62. The resource is returned to the requesting browser 51. Otherwise, if the URL must be encrypted, the process moves to step 58. In block 58, the encrypted URL value is calculated or determined (via data base lookup, file lookup, etc.). Once the value is determined, the process moves to block 59. The new, encrypted URL is returned to the browser via a redirect procedure. This return of the URL will tell the browser to issue a new request using the new, encrypted URL. This URL return can alternatively be done by returning a page to the browser with a link to the resource using the new URL along with or without a message.

Id. at 6:64-7:8.

72. Read in light of the specification and other claim limitations, a POSITA would easily understand this limitation in its plain meaning. The computer determines how the URL contained in the original resource request should be returned to the user (*e.g.*, through a web browser), and in particular, if the returned URL may be encrypted in full, partially, or not at all.

E. "determining[, by the computer,] whether the URL of the requested resource is required" – '419 Patent, claims 2 and 11; '634 Patent, claim 2

73. I understand that Defendants contend that this term is indefinite, and that Plaintiff contends it should be accorded its plain meaning.

74. This claim limitation is found in both the '419 Patent, claims 2 and 11 and the '634 Patent, claim 2. A POSITA would understand this claim limitation from the claim language itself, the preceding claim limitations, and support of this plain claim language in the specification.

75. For example, in both the '419 and '634 Patents' Claim 1, a resource request is received by the computer that contains a URL. The computer determines whether to encrypt that

URL. The computer determines whether the resource request is available and the computer locates the requested resource. Claim 2 of both patents "occurs after" this determination and starts by determining whether the requested resource (the subject of the resource request – the resource itself) should be encrypted.

76. A POSITA would understand that this claim term is relevant to the instance where the requested resource should be encrypted and reflects the computer further determining whether to include the URL along with the requested resource to the destination (*e.g.*, a user through a web browser) that requested the resource (*e.g.*, web page), which is clear from the plain meaning of the claim language.

77. The specification is clear that a URL may not be included along with the requested resource for various reasons:

> [T]he requested URL cannot be returned to the browser because: a) the resource is not available, b) the resource is truly not present (i.e. 404 type of error, from step 54 and step 61, c) the resource was requested via plain text and this is not allowed (from block 55) or d) because the encrypted URL could not be decrypted (from block 60).

Id. at 7:9-18.

F. "substantially real-time" / "substantially real-time data" – '518 Patent, claims 1, 10, and 17

78. I understand that Defendants claim that these phrases are indefinite, and that Plaintiff contends that these terms should be construed to mean "without intentional delay, given the processing limitations of the system."

79. The POSITA would understand that, in digital systems, there is no such thing as exactly "real-time" processing. For example, propagation delays in integrated circuits can cause extremely slight delays in processing signals from input to output. The POSITA would understand that systems which do not intentionally add delays are still considered "real-time" in this field of

invention, even if there are slight delays between input and output.

80. The '518 patent claims the collection of status information from mobile devices. Claim 1, for example, requires "wherein the status information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner." '518 Patent, claim 1. In this context, since the patent is discussing and claiming collecting information from mobile devices, the POSITA would have understood at the time of the invention that there may be delays introduced, for example, by high traffic on the mobile network. There may also be other delays that interfere with the collection of status information, such as transmission delays themselves. But the POSITA would understand that, as long as no intentional delays are added by the system, it is still a "substantially real-time" system.

81. I also understand that claim 1 of the '518 patent recites that "rules can be substantially uniformly applied to the status information," and Defendants do not contend that this use of the term "substantially" renders claim 1 indefinite. It is unclear how, according to the Defendants, a POSITA would understand "substantially uniformly" to be definite while simultaneously not understanding the scope of "substantially real-time [data]."

82. In my opinion, this claim phrase is not indefinite, as the POSITA would understand that the word "substantially" does not render the claim indefinite.

83. In addition, the POSITA would understand that "substantially real-time" means "without intentional delay, given the processing limitations of the system."

84. I have been informed that extrinsic evidence such as dictionary definitions can be used to understand how the POSITA would have been informed about the meaning of certain terms at the time of the invention. The 2004 edition of the Wiley Electrical and Electronics Engineering Dictionary defines "real time" as "That which occurs instantaneously, or so quickly that

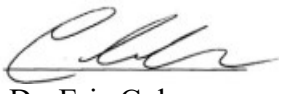
processing, entering, adaptation, or any other response is [at] least as fast as a triggering event or circumstance." I also understand that the Oxford English Dictionary defines "real time" in the context of computing as "the actual time during which a process or event occurs, esp. one analysed by a computer, in contrast to time subsequent to it when processing may be done, a recording replayed, etc."

85. Each of these definitions would have been understood by the POSITA, who would have understood that real-time means "instantaneous" or "without intentional delay," but what is or is not "real time" must be understood within the processing limits of the system. As discussed above, for example, mobile networks may be considered "real-time" even if information takes several seconds (or more) to be collected from mobile devices due to network traffic. Because the system is not intentionally delaying the data (e.g., not storing it for processing later), the system is considered "real-time."

VI. CONCLUSION

I declare under penalty of perjury that the foregoing is true and correct.

Dated: July 13 , 2023



Dr. Eric Cole

ATTACHMENT A

Dr. Eric Cole, Ph.D.

Cybersecurity, Networking, Computer, and IT Expert

44651 Provincetown Drive,
Ashburn, VA 20147

Cell Phone: (703) 909-2998
Email: ecole@secure-anchor.com
www.secure-anchor.com/expert-witness

Expert Overview

Dr. Eric Cole, Ph.D. is a cybersecurity, networking, computer, and information technology (IT) expert who has built a solid reputation in the information technology industry over the last three decades. His educational experience includes a master's degree in computer science from the New York Institute of Technology, and a doctorate in network security from Pace University. Dr. Cole's expert involvement in the information technology industry is demonstrated by his appointment as the commissioner on cybersecurity for the 44th president, holding a position as a senior fellow at SANS, and being elected to the Purdue University Executive Advisory Board. The accomplishments he has earned include an induction into the Information Security Hall of Fame, and he has been awarded as a Cyber Wingman from the US Air Force. Aside from his seasoned technical expertise, he is an author of various publications, like his recently released book, Cyber Crisis, which debuted at #1 on the Wall Street Journal's Best-Sellers List. Dr. Cole's expertise and experience includes working with both plaintiff and defense counsel as a cybersecurity, networking, computer, and IT expert.

Types of Cases

As an expert witness, Dr. Cole provides valuable insights and technical expertise for several types of cases. Below is a list of selected, sample case types:

- Apportionment
- Infringement & Non-Infringement
- Validity & Invalidity
- Trade Secrets
- Data Breaches

Areas of Expertise

As an industry-recognized expert, with over 30 years of firsthand experience, he has built a solid background and knowledgeable insight in several areas of technology. Below is a list of selected, sample areas of expertise:

- Cybersecurity
- Networking
- Operating Systems
- E-Commerce
- Web Technologies
- Protocols and Communications

Professional Experience

Secure Anchor Consulting Services: 2005-Present
Founder and CEO
Provides consulting services to Fortune 500, Fortune 50, financial institutions, international organizations, and the federal government. Employs innovative technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide security solutions.

SANS (Sysadmin Audit Network Security): 1999-2019
Director of the Cyber Defense Initiative
Lead instructor and course developer for several security courses, including the top selling courses. One of the highest rated instructors and one of the few instructors teaching a variety of courses. Executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW). Responsible for staying up on technology and developing new course material covering the state of the art in networking, information technology, and security. Created and led several key efforts including the Level One Notebook, Top 10/20 Vulnerability List, and the Cyber Defense Initiative, which included authoring the Critical Controls for Effective Cyber Defense. Developed business plans and created new technological initiatives. Constantly researched, assessed, and evaluated new security products and research efforts.

STI (SANS Technology Institute): 1999-2015
Dean of Faculty
A member of a five-person team tasked with creating a degree-granting educational institution and obtaining certification from the state of Maryland. Offered two master's degree programs focused on technical people needing managerial skills and managers needing technical skills. Designed and implemented curriculum and provided leadership to faculty. STI successfully received accreditation from the state of Maryland.

McAfee: 2009-2011
SVP, CTO of the Americas
As McAfee's visionary and evangelist, responsible for strongly influencing the company's strategic and technical direction, development, and growth as the global leader in digital security solutions. Key leader in the execution of technology strategy for platforms, partnerships, and external relationships. Worked closely with CEO, EVP of Product Operations, and other key stakeholders to establish a product vision and road map to achieve McAfee's goals and focused on identifying and capturing intellectual property and driving innovation across the company.

Lockheed Martin: 2005-2009
IS&GS Chief Scientist LM Senior Fellow
The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. Dr. Cole was selected by Lockheed Martin for its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. As a Lockheed Martin Senior Fellow (the first Fellow within Lockheed Martin's Information Technology Division), he was a frequently invited speaker at a variety of conferences and security events. As Lockheed Martin Chief Scientist, performed research and development to advance the state-of-the art in information systems security. Specialized in secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. Played a lead technical advisory role in many high-profile, security-focused projects for Federal clients to include civil, Intel and Department of Defense, including the FBI Sentinel, DHS Eagle, JPL, Hanford, and FBI IATI programs.

The Sytex Group, Inc. (TSGI): 2001-2005
Chief Technology Officer (CTO)
Positioned the company to achieve corporate growth and meet financial targets by utilizing and

enhancing technology. Worked as an executive team member to determine and implement technical direction and focus of company. Experience with running projects including managing development efforts to exceed client requirements. Created an intellectual property portfolio that included patents, journals, books, and white papers, resulting in an overall increase in market value and customer engagement. The efforts of the research team's intellectual property increased advertising, market share and customer satisfaction through conferences, proposals, and magazine articles. Maintained full accountability for revenue of $55 million and was indirectly involved in revenue of over $80 million. Provided continuous leadership to a research team of over twenty people creating intellectual property that surpassed teams twenty times their size. Yearly patents were in line with the top one thousand producing patent companies in the United States.

Developed and executed creative techniques for influx of technology into non-technical business units to drive revenue and profit. Interfaced with government officials, including the Pentagon, The White House and Capitol Hill, and corporate executives to identify critical network security problems that needed to be addressed and researched.

GraceIC: 2000-2001
Chief Security Officer (CSO)
Designed and executed strategy for establishing GraceIC as a leader in the network security arena. Developed the product line and built the services. Managed and directed security employees. Provided leadership and implemented internal security infrastructure, such as secure email, proper protection of data and security policies. Presented at national and international conferences and authored several articles. Performed and documented research into the area of future applications and solutions to the network security problem existing in the current market. Trained salespeople, program managers and engineers on how to sell, manage, and deliver security services. Maintained a pulse on technology in the marketplace to produce market plans.

American Institutes for Research: 1999-2000
Chief Information Officer (CIO)
Brought in to fix and revamp the entire IT infrastructure based on the organization having experienced several security breaches, virus outbreaks and unreliable performance on the network. Within three months, stabilized the entire IT infrastructure and within nine months rebuilt the entire infrastructure. Designed the network to achieve a balance between functionality and security while minimizing the monetary impact to the organization. After one year, there were no severe security breaches, and all attempted breaches were contained prior to causing any significant monetary loss. Virus problems were contained and controlled, and network uptime was 99.999%. Security and performance increased while overall IT costs were reduced by 15%. In addition, provided technical support for DARPA-sponsored research projects. Helped invent technology and innovation that lead to a spin-off company, Pynapse, which created a state-of-the-art intrusion detection system known as Checkmate that was later sold to SAIC.

Vista Information Technologies: 1998-1999
VP of Enterprise Security Services
Developed the Enterprise Security Services Group and was responsible for all internal and external security issues. Tracked and managed separate profit and loss center for security. Grew the team from one person to over twelve people and executed several million in annual revenue in less than a year. Set up the security and other monitoring services for the NOC/SOC. Created all security services offerings and generated all necessary marketing and sales material. Followed and assured compliance with business plan and financial tracking of security group. Performed security assessments and consulted on all areas of security. Designed, implemented, and monitored security solutions including firewall design, intrusion detection, vulnerability assessment and penetration testing. Performed evaluation and analysis of security tools and provided technical recommendations and product improvements for VC funded startups. Key presenter at Cisco sponsored security seminars around the country and performed partnership activities with Fortune 500 organizations.

Telligent: 1996-1998

Director of Security
Created and managed IT Corporate Security Department. Pivotal point of contact for all security concerns. Evaluated strategic plans and operational activities by performing risk assessment and determining how it might impact corporate security. Designed security solutions to meet operational needs. Integrated security and helped create NOC to provide proper monitoring of network. Developed the company's security policy and all required security guidelines. Set up lab to accurately assess and enhance the security features of the network. Performed and executed several computer investigations. Assisted and advised the legal department on laws, regulations, and policies relating to computer and information security. Evaluated several secure email solutions and installed PGP company wide. Established and set up web traffic monitoring and password tracking systems.

Central Intelligence Agency: 1991-1996
Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services
A Senior Officer of the agency that implemented the Internet Program Team that specialized in rapid development and in exploiting the latest Internet technologies to meet customers' requirements. The team designed, developed, assessed, and deployed products over three-to-six-month intervals. Designed and developed several secure communication systems. Responsible for providing technical direction, technical design, security assessment, and programming modules. Secured internal servers, continually performed intrusion detection, and reviewed audit logs. Performed independent security reviews and penetration testing of Internet servers (World Wide Web) for other offices. Identified several weaknesses and devised ways to fix those problems and secure the system. Received letter of appreciation from the Director of Central Intelligence (DCI) and six Exceptional Performance Awards.

Computer Engineer with Office of Security
Member of the information security assessment team. Evaluated and performed security assessment of network operating systems. Identified potential vulnerabilities and ways to secure the holes. Designed a large-scale auditing system with automated review capability. Worked on several virus investigations.

Education

Doctorate in Network Security, Pace University (2004)
Master of Science in Computer Science, New York Institute of Technology, Honors. (1994)
Bachelor of Science in Computer Science, New York Institute of Technology, Honors. (1993)

Certifications

Certified Information Systems Security Professional (CISSP)
Created several of the Global Information Assurance Certification (GIAC) programs and exams.

Organizations / Associations

Association for Computing Machinery (ACM)
Institute of Electrical and Electronics Engineers (IEEE)
Computer Security Institute (CSI)
Information Systems Security Association (ISSA)
International Computer Security Association (ICSA)
International Who's Who in Information Technology Common Vulnerability and Exposures (CVE)
HoneyNet Project - member (by invitation only)

Publications

1. Eric Cole. *Cyber Crisis.* BenBella Books, 2021.
2. Eric Cole. *Online Danger: How to Protect Yourself and Your Loved Ones from the Evil Side of the Internet.* Morgan James Publishing, 2018.
3. Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress, 2012.
4. Eric Cole. *Network Security Bible.2nd Edition.* Wiley, 2009.
5. Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollman, and Rachelle Reese. *Wiley Pathways Network Security Fundamentals Project Manual.* Wiley, 2007.
6. Eric Cole and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress, 2006.
7. Eric Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* Wiley, 2003.
8. Eric Cole. *Hackers Beware: The Ultimate Guide to Network Security.* New Riders/Sams Publishing, 2001.

Recent Expert Witness Experience

Adventist Health System Sunbelt Healthcare Corporation v. RxCrossroads, LLC, d/b/a Covermymeds, LLC, United States District Court Middle District of Florida (Orlando Division),

Case No. 6:22-CV-880-PGB-LHP

Provided Expert Declaration Services for Plaintiff Adventist Health System Sunbelt Healthcare (2023).

Celgard, LLC v. Shenzhen Senior Technology Material Co., et al., United States District Court Northern District of California,

Case No. 19-cv-05784-JST

Provided expert report services for plaintiff Celgard, LLC.

K.Mizra, LLC, v. Cisco Systems, Inc., United States District Court for the Western District of Texas (Waco Division),

Case No. 6:20-cv-01031-ADA

Provided expert report and deposition services for plaintiff K.Mizra LLC.

Future Field Solutions, LLC, et al. v. Erik Van Norstrand, Circuit Court for Howard County, Maryland,

Case No. C-13-CV-22-000581

Provided expert report services and participated in hearing for plaintiff Future Field Solutions,

LLC.

Janssen Products, L.P. v. eVenus Pharmaceuticals Laboratories, Inc., United States District Court for the District of New Jersey,

Case No. 3:20-cv-09369-ZNQ-LHG

Provided expert declaration services for plaintiff Janssen Products, L.P.

In the Matter of Certain Computer Network Security Equipment and Systems, Related Software, Components Thereof, and Products Containing Same, United States District Court for the Eastern District of Virginia (Norfolk Division),

Inv. No. 337-TA-1314 (ITC).

Provided an expert report, declaration, and testimony on behalf of plaintiff Centripetal Networks (2023).

Virtru Corporation v. Microsoft Corporation, United States District Court for the Western District of Texas Waco Division,

IPR No. IPR2023-00019

Provided expert declaration services for plaintiff Virtru Corporation.

Ivanti, Inc. v. Patch My PC, LLC, United States District Court for the District of Colorado,

Case No. 1:22-cv-00643-RMR-SKC

Provided declaration and deposition services for plaintiff Ivanti, Inc.

Genesis 1 Oil Services, LLC v. Wismann Group LLC, United States District Court for the Central District of California,

Case No. 8:20-cv-02114-SSS-ADS

Provided expert declaration services for plaintiff Genesis 1 Oil Services LLC.

Palantir Technologies Inc. v. Marc L. Abramowitz, United States District Court for the Northern District of California (San Jose Division),

Case No. 5:19-cv-06879-BLF

Provided expert reports, trial prep, and deposition services trade secrets (2022).

CUPP Cybersecurity LLC, et al. v. *Trend Micro, Inc., et al.*, United States District Court for the Northern District of Texas (Dallas Division),

Case No. 3:18-cv-01251-M

Provided expert reports and deposition services for plaintiff CUPP Cybersecurity LLC.

Sarah Freele v. ADT, LLC, United States District Court for the Northern District of Texas (Dallas Division),

Case No. 3:21-cv-01104-X

Provided expert report data breach and data compromise (2021).

Unified Patents, LLC v. Monarch Networking Solutions, LLC, United States Patent and Trademark Office,

Case No. IPR2020-01708

Provided expert declaration (2022).

Sunstone Information Defense v. International Business Machines Corporation, United States District Court for the Western District of Texas (Waco Division),

Case No. 6:20-cv-01033-ADA

Provided expert reports, depositions, demonstrations, and testimony on behalf of plaintiff Sunstone Information Defense (2022).

Boston Scientific Corp., et al. v. Nevro Corp., United States District Court for the District of Delaware (Wilmington),

Case No. 1:18-cv-00644-CFC-CJB

Provided opening report and deposition trade secrets (2018).

Shana Doty v. ADT, LLC d/b/a ADT Security Services, United States District Court for the Southern District of Florida (Fort Lauderdale Division),

Case No. 20-cv-60972

Provided expert witness consulting services, expert report, and deposition services on behalf of plaintiff Shana Doty (2020).

United States of America v. Lucy Xi, United States District Court for the Eastern District of Pennsylvania,

Criminal Action: 16-22-5

Provided expert witness consulting services on behalf of defendant Lucy Xi (2021).

Centripetal Networks, Inc. v. Lookingglass Cyber Solutions, Inc., et al., United States District Court for the Eastern District of Virginia (Richmond Division),

Case No. 3:21-cv-000597

Provided expert witness consulting services on behalf of plaintiff Centripetal Networks, Inc. (2022).

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. v. Communication Technologies, Inc., United States Patent and Trademark Office,

Docket No. 9843-0140IP1

Provided expert declaration services for plaintiff Samsung Electronics Co., Ltd.

WSOU Investments, LLC d/b/a Brazos Licensing and Development v. F5 Networks, Inc., United States District Court for the Eastern District of Virginia (Alexandria Division),

Case No. 3:20cv724

Provided expert reports and deposition services for plaintiff WSOU Investments.

Trustees of Columbia University in the City of New York v. Nortonlifelock, Inc., United States District Court for the Eastern District of Virginia (Richmond Division),

Case No. 3:13-cv-00808

Provided expert reports, depositions, demonstrations, and testimony on behalf of plaintiff Trustees of Columbia University in the City of New York (2022).

Appian Corporation v. Pegasystems Inc. and Youyong Zou, Fairfax County Circuit,

Court Case No. 2020-07216

Provided expert reports, depositions, demonstrations, and testimony on behalf of plaintiff Appian Corporation (2022).

Sprint Communications L.P. v. Charter Communications Inc., et al., United States District Court of Kansas (Kansas City),

Case No. 2:20-cv-02161

Provided expert witness consulting services on behalf of defendant Charter Communications Inc. (2021).

Root Insurance Co. v. Genpact (UK) Ltd., JAMS Arbitration

REF. No. 1450007525

Provided expert reports, depositions, and arbitration support on behalf of respondent Genpact (UK) Ltd. (2022).

Securities and Exchange Commission v. Zhoubin Hong, et al., United States District Court for Central District of California,

Case No. 2:20-cv-04080-MCS

Provided expert report on behalf of the plaintiff Securities and Exchange Commission (2021).

Synopsys, Inc. v. Risk Based Security, Inc., United States District Court for the Eastern District of Virginia

(Richmond Division),

Case No. 3:21-cv-00252

Provided expert report, deposition, and demonstration on behalf of plaintiff Synopsys, Inc. (2022).

Cox Automotive, Inc., et al. v. The Reynolds and Reynolds Company, American Arbitration Association,

AAA Case No. 01-19-0000-4548

Provided expert report on behalf of respondent The Reynolds and Reynolds Company (2021).

Fortinet, Inc., v. Forescout Technologies, Inc., United States District Court for the Northern District of California (San Francisco Division),

Case No. 3:20-cv-03343-EMC

Provided expert declaration, expert report, and deposition services for plaintiff Fortinet, Inc.

Bitglass, Inc. v. Netskope, Inc. et al., United States District Court for the Northern District of California (San Francisco Division),

Case No. 3:20-cv-005216

Provided expert report on behalf of plaintiff Bitglass, Inc. (2020).

802 Systems, Inc. v. Cisco Systems, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:20-cv-00315-JRG

Provided expert declaration infringement and validity for plaintiff 802 Systems, Inc. (2020).

Fourth Dimension Software v. Der Touristik Deutschland GMBH, United States District Court for the Northern District of California,

Case No. 19-CV-05561-CRB

Provided expert report and deposition services for plaintiff Fourth Dimension Software.

Energy Intelligence Group, Inc. v. *Kirby Inland Marine, L.P.*, United States District Court for the Southern District of Texas (Houston Division),

Case No. 4:19-cv-03520

Provided expert report and deposition services for plaintiff Energy Intelligence Group, Inc.

Freshub, Inc., et al. v. Amazon.com, Inc., et al., United States District Court for the Western District of Texas (Austin Division)

Case No. 1:19-CV-00885-ADA

Provided expert report, deposition, and trial testimony services on behalf of plaintiff Freshub Inc., et al. (2021).

Finjan, Inc. v. Cisco Systems, Inc., United States District Court for the Northern District of California,

Case No. 5:17-cv-00072-BLF-SVK

Provided expert report and deposition testimony on behalf of plaintiff Finjan, Inc. (2020).

NexStep, Inc. v. Comcast Cable Communications, LLC, United States District Court for the District of Delaware,

Case No. 19-1031 (RGA)(SRF)

Provided expert reports and deposition services to plaintiff NexStep, Inc.

Unified Patents, Inc. v. Kioba Processing, LLC, US Patent Trial, and Appeals Board,

Case No. IPR2020-01695

Provided expert declaration on behalf of plaintiff Unified Patents, Inc. (2020).

Unified Patents, LLC, v. Biometric Associates, L.P., United States Patent and Trademark Office,

File No. 4910-101

Provided expert declaration services for plaintiff Unified Patents, LLC.

Mark Voelker v. BNSF Railway Company, United States District Court of Montana Missoula Division,

Case No. 9:18-CV-00172-DLC

Provided expert report on behalf of defendant BNSF Railway Company (2020).

Finjan, Inc. v. Qualys, Inc, United States District Court for the Northern District of California

Case No. 4:18-cv-07229-YGR

Provided expert report and deposition services for plaintiff Finjan, Inc.

BrandRep, LLC v. Ruskey, et al., Court of Chancery of The State of Delaware,

Case No. 2018-0541-SG

Provided expert report and deposition testimony on behalf of defendant Ruskey, et al. (2020).

Association of Owners of Kukui Plaza v. American Savings Bank FSB, Circuit Court of the First Circuit, State of Hawai'i,

Case No. 18-1-0660-05

Provided expert report on behalf of defendant American Savings Bank FSB (2020).

Finjan, Inc. v. SonicWall, Inc., United States District Court for the Northern District of California

Case No. 5:17-cv-04467-BLF

Provided expert report and deposition services for plaintiff Finjan, Inc.

Finjan, Inc. v. Rapid7, Inc. and Rapid7, LLC, United States District Court for the District of Delaware

Case No. 1:18-cv-01519-MN

Provided expert report and deposition services for plaintiff Finjan, Inc.

Centripetal Networks, Inc. v. Cisco Systems, Inc., United States District Court for the Eastern District of Virginia,

Case No. 2:18-cv-00094

Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Centripetal Networks, Inc. (2020).

Unified Patents v. TransactionSecure, LLC, United States Patent Trial and Appeals Board,

Case No. IPR2020-00321

Provided written declaration on behalf of the petitioner Unified Patents (2019).

Glenn Winder v. Marriott International, Inc., et al., Ontario Court of Superior Justice,

Case No. CV-1800611365-00CP

Provided written opinion on behalf of the plaintiff Glenn Winder (2019).

Fortinet, Inc. v. British Telecommunications Public Limited Company, United States Patent Trial, and Appeals Board,

Case No. IPR2019-01327 and IPR 2019-01328

Provided written declaration on behalf of the patent owner British Telecommunications (2019).

Finjan, Inc. v. Juniper Network, Inc., United States District Court for the Northern District of California,

Case No. 3:17cv5659

Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Finjan, Inc. (2019).

Vivian Deveroux V. Apple, Inc., Superior Court of the State of California County of Santa Clara,

Case No. 1-14-cv-271773

Provided expert report and deposition testimony on behalf of plaintiff Vivian Deveroux (2019).

United States of America v. Shan Shi, et al., United States District Court for the District of Columbia,

Case No. 1:17-cr-00110-CRC

Provided trial testimony on behalf of defendant Shan Shi, et al. (2019).

Colortokens, Inc. v. Medovich, United States District Court for the Northern District of California,

Case No. 3:18-cv-2444

Provided expert opinion on behalf of defendant Medovich. (2019).

Avepoint, Inc. v. Onetrust, LLC., Patent Trial and Appeals Board, Post Grant Review,

Case No. PGR 2018-00056

Provided expert report on behalf of plaintiff Avepoint, Inc. (2019).

Finjan, Inc. v. *ESET, LLC, et al.,* United States District Court for the Southern District of California,

Case No. 3:17-cv-0183-CAB-BGS

Provided expert report and deposition services for plaintiff Finjan, Inc.

Centripetal Networks, Inc. v. Keysight Technologies, United States District Court for the Eastern District of Virginia,

Case No. 2:17-cv-3836

Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Centripetal Networks, Inc. (2018).

Gubarev, et al. v. Buzzfeed, Inc., et al., United States District Court for the Southern District of Florida,

Case No. 0:17-cv-60426

Provided expert report on behalf of plaintiff Gubarev, et al. (2018).

Daniel Bennett v. Lenovo (Canada), Inc., et al., Ontario Superior Court of Justice,

Court File No. CV-15-00523714-00CP

Provided expert consultation on behalf of plaintiff Daniel Bennett (2018).

Finjan, Inc. v. Blue Coat Systems, Inc., United States District Court for the Northern District of California,

Case Nos. 5:15-cv-3295; 5:13-cv-3999

Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Finjan, Inc. (2018).

Zscaler, Inc. v. Symantec Corporation, United States Patent Trial, and Appeals Board,

Case No. IPR2018-00929

Provided written declaration on behalf of the patent owner Symantec Corporation (2018).

YLD Limited v. The Node Firm, LLC, et al., United States District Court for the Northern District of California (San Francisco),

Case No. 3:16-cv-399

Provided expert report and deposition testimony on behalf of defendant The Node Firm, LLC, et al. (2017).

Phishme, Inc. v. Wombat Security Technologies, Inc., United States District Court of Delaware,

Case No. 1:16-cv-403

Provided expert report, deposition testimony, and supplemental expert report on behalf of plaintiff Phishme, Inc. (2017).

Smith, et al. v. Federal Title & Escrow Company, et al., United States District Court for the District of Columbia,

Case No. 1:17-cv-1580

Provided expert opinion on behalf of plaintiff Smith, et al. (2017).

Unified Patents, Inc. v. Universal Secure Registry, LLC, US Patent Trial, and Appeals Board,

Case No. IPR2018-00067

Provided expert declaration, deposition testimony, and supplemental expert declaration on behalf of plaintiff Unified Patents, Inc. (2017).

BASCOM Global Internet v. AT&T Mobility, LLC, United States District Court for the Northern District of Texas,

Case No. 3:14-cv-03942

Provided expert report on behalf of the defendant AT&T Mobility, LLC. (2017).