UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

- - - - - - - - - - - - - x

PALO ALTO NETWORKS, INC.,

Petitioner,

v.

BT AMERICAS INC.,

Patent Owner.

- - - - - - - - - - - - - x

Case IPR2023-00889

U.S. Patent No. 7,895,641

Deposition of WENKE LEE, PH.D.

New York, New York

Thursday, April 4, 2024

8:58 A.M.

Job No.: 531852

Pages: 1 - 297

Reported By: Anita M. Trombetta, RMR, CRR

PAN EX1046
Palo Alto Networks v. BT Americas
IPR2023-00889

Deposition of WENKE LEE, PH.D., held at the offices of:

Proskauer Rose LLP
Eleven Times Square
New York, NY 10036-8299
212.969.3000

Before Anita M. Trombetta, RMR, CRR, Notary Public in and for the State of New York.

A P P E A R A N C E S

ON BEHALF OF THE PETITIONER:

JONATHAN TUMINARO, ESQUIRE
DANIEL S. BLOCK, ESQUIRE
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 New York Ave, NW
Washington, DC 20005
202.371.2600

ON BEHALF OF THE PATENT HOLDER:

NOLAN GOLDBERG, ESQUIRE
EDWARD WANG, ESQUIRE
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036-8299
212.969.3000

----------I N D E X----------

WITNESS

WENKE LEE, PH.D.

EXAMINATION BY PAGE

MR. TUMINARO 5

----------E X H I B I T S----------

(NO EXHIBITS MARKED.)

P R O C E E D I N G S

W E N K E L E E, PH.D.,

called as a witness, having been duly sworn by a Notary Public, was examined and testified as follows:

EXAMINATION BY

MR. TUMINARO:

Q Good morning, Dr. Lee. Jonathan Tuminaro. Nice to meet you.

You have in front of you Exhibit 2016. And do you recognize this document?

A Yes.

Q It's your declaration in this IPR proceeding.

A Yes.

Q And if you go to the last page of Page 107, is that your signature?

A Yes.

Q And you signed this declaration on or about February 21, 2024.

A Yes.

Q Anything you want to change in your

declaration?

A No.

Q And nothing you want to add, nothing you want to delete?

MR. GOLDBERG: Objection to form.

BY MR. TUMINARO:

Q Nothing you want to add?

A Not at this point.

Q Nothing you want to delete?

A Not at this point.

Q Okay. And you also have in front of you Exhibit 1001. It's a '641 -- U.S. Patent Number 7,895,641.

A Yes.

Q And if I refer to it as the '641 patent, you'll understand what I'm talking about?

A Yes.

Q You've seen the '641 patent before?

A Yes.

Q Okay. Let's look at the claim. So Claim 1 is directed to a system for operating a probe that's part of a security -- remote security

monitoring system; is that right?

MR. GOLDBERG: Objection to form.

A It says, "A probe is part of a security monitoring system of a computer network." It doesn't say remote.

Q Oh, okay.

You know what a security monitoring system is, right?

A Given context, yeah. I mean, different people apply to different situation. Yeah, I know security monitoring.

Q What's a security monitoring system?

MR. GOLDBERG: Objection to form.

A Are you asking in the context of this patent or just in general?

Q Well, I'm asking what -- do you know what a managed security monitoring system is?

MR. GOLDBERG: Objection. Asked and answered.

A Again, I know in general, but again, are you asking in the context of this patent or just in general, general knowledge?

Q So right now I'm asking in general.

Do you know what a managed security monitoring system is?

A Okay. So I mean, I can use Figure 1 of the patent as example. Again, as an examples, so with it -- put these answers in the context of this patent, right? So on the left side, you have the security monitoring systems on the client side, customer side.

On the right-hand side, you have the SOC, secure operation center, and you see the pipes between left and right. So information, I think, according to the claim, that would be some sentry information is being passed from the customer side to the right-hand side. The sentry do more analysis on the right-hand side by the security operation center.

And if you look at Figure 1, there is a SOCRATES, and basically problem and expertise management system. So that's example of managed monitoring -- security monitoring system.

Q Okay. And then in Claim 1, one of the

things that Claim 1 requires are probes to collect status data; is that right?

A Let me look at the claim language. Yeah. So 1A says, "A censor coupled to collect status data from at least one monitored component of the network."

Q And then the claim -- there is a first level of analysis by the filtering subsystem that performs filtering and an analysis of the post-filtering residue; is that right?

MR. GOLDBERG: Objection to form.

A So claim 1B says, "A filtering subsystem coupled to analyze -- to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering, followed by an analysis of post-filtering residue.

Q Yeah, I know what the claim says. I guess my question is: Would you consider that a first level of analysis that's performed by the filtering subsystem?

MR. GOLDBERG: Objection to form. Scope.

A What do you mean by first level?
Q Well --
A I mean, that's not -- new term that I'm not seeing in the patent. Unless you point it to me, what's first level, what's second level.
Q All right. Well, does the claim require a first level of analysis and a second level of analysis, in your opinion?
MR. GOLDBERG: Objection to form and scope. Outside the scope.
A Again, point me to where in the patent talks about what is first level, what is second level.
Q I'm sorry. What I'm asking -- maybe I'm not clear. What I'm asking about is your -- in your opinion.
In your opinion, does the claim require a first level of analysis and a second level of analysis?
MR. GOLDBERG: Objection to form. Outside the scope.
A Yeah, so all the opinions expressed in my

declaration, if the claim talks about -- if the patent talks about first level or second level I will opine on it. Since it did not, I did not opine.

Q Have you ever characterized the scope of the claim in the '641 patent as having a first level of analysis and a second level of analysis?

MR. GOLDBERG: Objection to form. Do you want to point him to something, Jonathan?

MR. TUMINARO: I want to ask him my questions.

A So again, like I said, my report expressed own opinion. If I had, you know, talked about first level, second level, and I cannot recall where it is, point me to it. Otherwise, if I'm not -- if I have not opined, that means I'm not rendering opinion.

Q Have you ever given an opinion on this patent in another context?

A I don't recall the details.

Q But have you offered a declaration on this patent in a different proceeding?

A I believe so, yes.
Q Do you believe -- do you recall ever characterizing the scope of Claim 1 as including a first level of analysis and a second level of analysis?
A I don't recall.
Q You don't recall doing that?
A No.
Q Okay. After the filtering subsystem -- going back to Claim 1 -- well, information about potentially security-related events is transmitted to an analyst for analysis; is that right?
MR. GOLDBERG: Objection to form.
A Can you point me to a specific limitation in the Claim 1?
Q Claim Element 1C.
A Okay.
Q What does that mean to you?
MR. GOLDBERG: Objection to form. Outside the scope.
A Yeah, it says, "A communication system coupled to transmit information about the

identified -- identified events to analysis system associated with the security monitoring system."

Q Right. So my question to you -- I can read the claim -- do you understand that claim limitation to require that information about potentially security-related events are transmitted to an analyst system for analysis?

MR. GOLDBERG: Objection. Outside the scope. Form.

A So I mean that's what the claim language says, you know, communication system will transmit information about identified events to an analysis system associated with the security monitoring system.

Again, we can refer to Figure 1 to basically, you know, talks about left side. So the Figure 1 that's left side will be on the customer side doing the monitoring and the right-hand side doing some, you know -- some additional filter analysis and there's a pipes communication system in between to -- to -- to transmit the information about the identified

events to analysis -- to another system. So yeah.

Q So I appreciate that I think you were trying to answer my question, but I don't know that you actually did.

Do you understand claim element 1C to require that information about a potentially security-related event is transmitted to an analyst system?

MR. GOLDBERG: Objection. Form. Outside the scope. Asked and answered.

A So, again, claim 1C says, "A communications system coupled to transmit information about the identified events to an analysis system."

Q So my -- I know what the words say. My question is: What do you understand those words to mean?

MR. GOLDBERG: Same objections.

A That means -- sorry. That means plain old meaning, identify events. The event has been identified.

Q What are the identified events in the

claim?

A So we can go to the patent. I think it gave some examples.

Q Before you go --

MR. GOLDBERG: He's answering the question. Let him answer please.

MR. TUMINARO: I was going to try to help him out --

MR. GOLDBERG: Are you done with your answer?

THE WITNESS: Yeah.

A So, again, like I said, the patent gave some examples of those identified events.

Q How about this: After the transmitting in 1C, element 1C of the claim, would you agree that feedback is provided from a human security analyst to update the probe's analysis capability. Is that what's required in the claim?

MR. GOLDBERG: Objection to form.

A That's not according to the -- according to the Claim 1B -- 1D. According to Claim 1D, "A receiver for receiving feedback at the probe based

on empirically derived information reflecting operation of the security monitoring system."

So I didn't say the feedback is from a human analyst. I didn't say that.

Q So you think the claim doesn't require feedback from a human analyst?

MR. GOLDBERG: Objection to form. Misstates testimony.

A That's not what I said. 1D did not say -- did not explicitly say it has to be from a human analyst.

Q Does the claim require feedback from a human analyst?

MR. GOLDBERG: Objection. Scope.

A As I already said, 1D says, "A receiver for receiving feedback at the probe." I didn't say the feedback, you know, has to be from a human analyst.

Q So you don't -- you think the claim doesn't require a feedback from a human analyst?

MR. GOLDBERG: Objection. Form, asked and answered. Misstates the prior testimony.

A Again, like I said, 1D did not explicitly say human analyst.

Q So I know what the -- I'm trying to understand -- give you an understanding of how you would interpret the claim because you're offering opinions about whether the references to each certain claim elements, you're offering opinions about whether Counterpane's product meets certain claim limitations so I'm trying to get an understanding of what you understand the claim language to mean. Does -- do you get that?

MR. GOLDBERG: Objection to form.

A Like -- hopefully you also get my answer as well. I interpret -- I basically read the claim and opine the claim did not say the feedback from human analyst. Okay? So that's why I'm offering an opinion as they are stating in the report.

Q So you would -- it is -- is Claim 1 directed to operating a managed security monitoring service?

MR. GOLDBERG: Objection. Form. Scope.

A Can you repeat that question again?
Q Is Claim 1 directed to a system for operating a managed security monitoring service?
MR. GOLDBERG: Objection. Form. Scope.
A So if you read Claim 1, it did not explicitly say, this is for managed security monitoring system. It did not say so.
Q Well, have you heard of Counterpane Managed Security Monitoring System?
A Yes, I have.
Q Do you believe that Counterpane's -- and sometimes you refer to it as Counterpane's MSM; is that right?
A Yeah, probably -- yeah, I mean I don't recall exactly how I -- how I short-handed it, but yeah, I know about the product, yes. Yes, MSM, yeah, I put it in the.
Q Page 100, right?
A Yes.
Q Do you believe that counter panes MSM is an example of a system that will fall within the scope of Claim 1?

MR. GOLDBERG: Objection. Form. Outside the scope.

A So like I said, Claim 1 does not explicitly state that the system is for managed security monitoring system.

Q Do you believe that Counterpane's MSM is an embodiment of Claim 1?

MR. GOLDBERG: Objection. Form. Outside the scope. Asked and answered.

A So in my report, I mean, if you look at, I think Paragraph 213. So Paragraph 213, the last sentence I said, "Counterpane's MSM is an embodiment of the Schneier patent and is captured by the claims."

Q So does that mean that you believe in your opinion that Counterpane's MSM is an embody of Claim 1, of the '641 patent?

A So like I said, in the report, Counterpane is an embodiment of the Schneier patent and is captured by the claims.

Q So I could read what your declaration is. I'm trying to understand what the scope of your

opinion is. Is the Counterpane's MSM an embodiment of Claim 1?

MR. GOLDBERG: Objection. Asked and answered.

A So I already said it's an embodiment of the Schneier patent and it's captured by the claims. So it's Claim 1 part of claims already said in the report.

Q No, you didn't say it. I still don't know, is it an embodiment of Claim 1 or not?

MR. GOLDBERG: Objection. Argumentative.

A The claims -- the claims of the Schneier patent. That's what I said.

Q So are you saying that the Counterpane's MSM is an embodiment of every single one of the claims of the '641 patent?

A So I already said that it's captured by the claims. And I -- I didn't say exclude this one or only include this one. So it's clear as written.

Q Which is not clear to me because I don't know which claim it is embodies I'm trying to

understand?

MR. GOLDBERG: Objection argumentative. Decorum, please.

Q I'm trying to understand which claims you believe it's an embodiment of. I see that you say the claims, but I don't know which claims that you're saying it's an embodiment of. That is my question to you, with all due respect?

MR. GOLDBERG: Objection. Asked and answered.

A So we do all this back if there is an a need only exclude certain things I would say so, in the report. So my point is, my opinion is stated in the report. It's captured by the claims.

Q But do you have an opinion about whether Claim 1 captures an embodiment -- captures the Counterpane MSM?

MR. GOLDBERG: Objection. Asked and answered.

A So like I said, I already said that MSM is an embodiment of the Schneier patent and it's

captured by the claims. I didn't specify say which claim should be included in the sentence which claim should not be included in the sentence. It's clear as written. It's captured by the claims.

Q Is it captured by every single one of the claims?

A The claims of the Schneier patent, that's what it says here.

Q So every single claim in Claim 1 through 25, the -- the Counterpane's MSM falls within the scope of every single one of those claims; is that your opinion?

MR. GOLDBERG: Objection. Asked and answered. Misstates the prior testimony.

A So like I said, this is already clearly stated that it's captured by the claims. If you say, hey, what about that claim, this claim, that claim, then we can go into details of, you know, be specific about which limitation you want me to talk about. Otherwise, this statement basically is capturing my opinion that MSM is an embodiment

of the Schneier patent as captured by the claims.

Q Do you believe that the Counterpane's MSM meets every claim limitation of Claim 1?

MR. GOLDBERG: Objection. Form asked and answered.

A It already says so in the report.

MR. GOLDBERG: Wenke, you got to pause to let me object.

Q You said it's an embodiment of claims. What I'm asking, does it meet all the claim limitations of Claim 1, the Counterpane's MSM?

MR. GOLDBERG: Objection. Form, scope. Asked and answered several times.

A So I already answered here in -- also stated in the report, unless you say there is a different meaning by captured by the claims and then if you say, hey, you don't like the word capture, you don't like the -- the way that I use parallel for claim. I'm saying for me, it's as clear as stated and written in the report, is captured -- a MSM as the embodiment of the Schneier patent is captured by the claims. I

don't know how more clearer do you need? I mean, if you say, hey, this particular limitation, I have a problem, okay, let's discuss that. Otherwise, this statement captures my opinion already.

Q So let's take a look at Paragraph 214 of your declaration.

A Okay.

Q What's the purpose of that paragraph?

MR. GOLDBERG: Objection. Form.

A (Document review.)

Yeah, so that paragraph give you -- so basically say, "Counterpane MSM is a system for operating a probe as part of the security monitoring system for computer network. And that's the -- I don't know what you call it. It's a preamble of Claim 1, and also Claim 18.

Basically Claim 18 is a method claim. It talks about, essentially, how Counterpane -- basically saying that Counterpane carries out the claim method.

MR. GOLDBERG: Wenke, are you done

answering?

THE WITNESS: Yeah.

MR. TUMINARO: Are you done testifying?

MR. GOLDBERG: I wasn't testifying, but I was trying to give the witness a chance to answer the question. Since you jumped right in while he was still looking at the document.

BY MR. TUMINARO:

Q So in Paragraph 214, is the purpose of that paragraph to show that the Counterpane MSM meets the limitation of claim element -- meets the limitations of Claim 1 of the '641 patent?

MR. GOLDBERG: Objection to form.

A So 214, like I said, you know, the -- the first sentence talks about counter panes is a system for operating a probe as part of a security monitoring system for computer networks. That's Claim 1, right, and then also Claim 18 and then in the paren, I said Counterpane MSM carries out claim method. So just, you know, supporting my opinion that MSM, you know, is captured by the claims.

Q Right. So I understand that you said it's your opinion that -- that Counterpane MSM is captured by the claims. Then I asked you which one and what you said is, well let's look at the specific elements and we can talk about the specific elements. So now what I'm asking about is the specific elements. Is Paragraph 214 trying to show that the Counterpane MSM meets the specific claim elements of Claim 1. That's my question?

MR. GOLDBERG: Objection to form. Mischaracterizes the prior testimony. Asked and answered.

A So I think previously when I answered that in Paragraph 213, I said MSM is embodiment of the Schneier patent is captured by the claims. So that's been answered.

For this particular question that you're asking, I'm just, like I said, I'm reading the first -- the first sentence of Paragraph 214 and talks about MSM basically -- it basically meets Claim 1 and also meets the Claim 18 as way to

explain it further.

Q Do you show in Paragraph 214, or in any other paragraph in your declaration that the Counterpane MSM meets element 1A of the '641 patent?

MR. GOLDBERG: Objection. Form.

A So if you read the Paragraph 214, right, we basically talk about -- talk about MSM is a system for operating probe as part of the security monitoring system for computer network. That's the preamble of Claim 1. Then I also say see also Claim 18 and MSM carries out the claim method and you can just compare claim, Claim 18 and Claim 1. I mean, which -- which limitation you have -- you have problem? We can discuss that.

Q Didn't I just ask you about claim 1A?

A But what I'm trying to say is that Claim 18 is a method claim, right? So like I said, you know, which -- which limitation in Claim 1 that you don't think I have covered?

Q Have you used the Counterpane MSM before?

A No.

Q Did you analyze the Counterpane -- have you seen the Counterpane MSM used before?

A No.

Q Did you analyze the Counterpane MSM to form any of the opinions in your report?

MR. GOLDBERG: Objection to form.

Q In your declaration?

A So like I said, in Paragraph 215 through -- through -- yeah, through end. Basically, yeah, I mean I was aware of Counterpane. I actually know the inventor. I mean since 1998 I know what they're trying to do. So I can offer an opinion of the contextual information about MSM, how we, you know, people like me will understand what product MSM is doing and technologies behind it.

Q But you yourself have never used the Counterpane MSM, right?

A No.

Q You yourself has never seen the Counterpane MSM in use, right?

A No, not in use.

Q Did you analyze -- in your opinions are based on publicly available documents relating to the Counterpane MSM, right?

A Let me see how I cite some references.

So I mean, I actually in my report I cited various industry report or references in that -- around the time that Counterpane was founded or MSM, I mean the whole concept monitoring -- managed security monitoring concept was, you know, was formulated. Yeah, so -- so my point is that even though I don't -- I have not personally used it, I mean like I said, I know this technology as soon as you since the late 1990s. I remember Bruce Schneier was giving a talk at a conference I attended, yeah if I ask you if a personally used it. But if you ask me I do need to actually personally use it in order to refreshed my opinion, the answer is no, because I know this stuff. I actually cited references throughout my report to say, hey, look, I'm not the only one who know about this stuff.

Q You don't cite any technical documentation

how the Counterpane MSM works, right?

MR. GOLDBERG: Objection to form.

A Can you repeat the question again.

Q Technical documentation about the Counterpane MSM, you do not cite anywhere in your declaration, true?

MR. GOLDBERG: Same objection.

A I don't recall if you, you know, but, you know, I could be wrong. If you can give me the whole list of references I cited, I can double-check.

Q Before I get there, do you show that the Counterpane MSM meets claim limitation 1B of the '641 patent?

MR. GOLDBERG: Objection. Form.

A So in my report, I do not recall explicitly or specifically talking about 1B, but like I said, throughout my report I talk about, you know, MSM is embodiment of the Schneier patent and captured by the claims and, you know, I said it in Paragraph 213, paragraph 214, and then if you -- and then I repeat the same opinion in

Paragraph 220, basically, you know, Claim 1 through 27. And so on.

So essentially what I'm trying to say is that it basically, like I said, the same opinion I offer in -- in 213 that is, you know, the MSM is captured by the claims. I did not as I recall, I did not explicitly talk about 1B.

Q Okay. Do you show in your declaration that the Counterpane MSM meets the limitations of element 1C of the '641 patent?

MR. GOLDBERG: Objection. Form.

A So like I said, I offer opinion at the last sentence in Paragraph 2 and to say Counterpane MSM is an embodiment of the Schneier patent is captured by the claims. With that, I did not have to specifically go into limitation by limitation. At least I don't recall doing that, but like I said, my opinion has already been captured by this sentence.

Q So you think it's sufficient that you have this single sentence that says you believe it's an embodiment examine that's enough to show that the

Counterpane MSM meets the claims?

MR. GOLDBERG: Objection. Form, misstates testimony, argumentative. Asked and answered.

A So like I said, that's -- that's my opinion offered in the report. I also gave the, you know, context of Counterpane and then emphasized that meets the claim. You know, if you say it's sufficient or not, of course I or an opinion about in the report if you think it's not sufficient, then tell me why it's not sufficient. You want me to go into every single limitation you think is not sufficient, we can talk about that.

Q So you said earlier that you know that the Counterpane MSM really well.

A Hold on, when did I say that, exactly when I use the words really well? Do I say that? Do I say that? Do I say -- no, I said -- did I say I know MSM really well? Did I say that?

MR. GOLDBERG: I'll just object. Mischaracterizes the prior testimony.

BY MR. TUMINARO:

Q Let me ask you, do you think you know the

Counterpane MSM very well?

A Can you repeat the question again?

Q Do you think you understand the functionality of Counterpane MSM very well?

MR. GOLDBERG: Objection to form.

A And do you mean what by functionality?

Q Do you understand how the Counterpane MSM works?

MR. GOLDBERG: Objection to form.

A Like I said, I know the technology behind it in general.

Q Do you know the name of the feature of the Counterpane MSM that meets limitations of element 16 of the '641 patent?

MR. GOLDBERG: Objection to form. Outside the scope.

A I don't recall its specific features, you know, product module names.

Q Do you know the name of the feature of the Counterpane MSM that meets the limitations of element 1B of the '641 patent?

MR. GOLDBERG: Objection to form. Outside

the scope.

A So like I said, I already offered an opinion in Paragraph 213 and then throughout the my report starting in paragraph 213 I did talk about various aspects of the technology that, you know, meets, you know, the claims. Yeah, I mean that's -- that's -- that's, you know, like I said, those are my opinions already captured in the report.

Q Well, in Paragraph 214 on Page 101 there is a sentence that says, "The sentries collect data from network devices and utilize over 20,000 filters to filter potentially security threats -- potential security threats."

Do you see that?

A I'm sorry, which paragraph again?

Q Paragraph 214?

A Okay.

Q Page 101?

A Okay.

Q The three lines down from the top?

A Okay.

Q Toward the middle of the page, it says, "The sentries collect data from network devices and utilize over 20,000 filters to filter potential security threats."

Do you see that?

A Yeah, I see the sentence, yes.

Q Have you shown that the Counterpane MSM includes a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering?

MR. GOLDBERG: Objection to form. Outside the scope.

MR. TUMINARO: How is that outside the scope?

MR. GOLDBERG: It's outside the scope of his opinion, which is right in front of you.

You can smirk and laugh all you want.

MR. BLOCK: Your position is it's if it's

not in the report, it's outside the scope. We're not allowed to ask him questions about what's in the report?

MR. GOLDBERG: He did not offer the opinion what you're questioning about. You can ask the question, but I'm objecting it's outside the scope.

MR. BLOCK: So to be clear, your expert did not offer an opinion that it meets a particular element of the claim? Is that what your position is?

MR. GOLDBERG: I'm not testifying.

MR. BLOCK: You just said it. Sounds like you are.

MR. GOLDBERG: I think you're mischaracterizing what I said.

A So like I said, in Paragraph 214, I talk about MSM is embodiment the Schneier patent is captured by the claims. And 214 later on it says the centuries collect data from network devices and utilize over 20,000 filters to filter potential security threats, right, and then the

next sentence say the sentry also uses analysis engine to further analyze post-filtering residue, which is then sent to the SOC and SOCRATES.

Q I understand that you said that, right, but what I'm saying is have you shown that the Counterpane MSM does positive filtering, negative filtering, and has a residue that's leftover, like in element 1B of the '641 patent?

MR. GOLDBERG: Objection. Form.

A So like I said, this sentence says about the sentry also utilizes analysis engine to further analyze post-filtering residue, post-filtering residue.

Q But where have you shown what reference teaches you that the Counterpane MSM actually has post-filtering residue?

MR. GOLDBERG: Objection. Form. Scope.

A Because here I cite reference 2009, I guess paragraph 12.

Q You've been handed what was previously marked as Exhibit 2009, which you cite. If we go to Page 12, can you show me what on that page is

teaching that the Counterpane MSM creates a post-filtering residue?

A So here -- (document review.)

Okay. So what I said here is that -- so basically Page 12 talks about the sentry, and so, basically, it says it is capable of processing millions of messages per day, you know, including from all devices on your network, including those that see internal threats. The filters -- the sentry filters data it collects using adaptive and proprietary set of rules, correlate that data with data from other devices and previous data. And sends an encrypted -- sorry, sends the results via an encrypted tunnel to one of our secure operations centers.

So that's the high level view of the sentry needs to process all data and then doing, you know, adaptive, and call it -- adaptive analysis correlation using a bunch of rules, including using data from other devices and previous data. So a person of ordinary skill in the art would understand that's what normally you

would do as filtering analysis.

And actually, in the paragraph -- sorry, page, I'm trying to see -- yeah, so basically Page 15, it goes more -- more into detail of what sentry is doing. So again, it talks about the breadth of the coverage, monitoring, meaning -- passive means this captures the data in particular as the Schneier patent talks about, capture the status data from the network traffic, and then -- and then has a re -- very broad coverage, broad, broader than traditional intrusion detection system.

Yeah. So basically go into more detail to talk about the amount of data and the need to correlate information from -- from multiple censors.

So I think that really matches what the -- what Figure 1 -- of the -- in terms of architecture, right, then talks about sending data to SOC. That's really, you know, fits the Figure 1, you know, Figure 1 captures that very nicely. And then -- and then go to Figure 2,

essentially, a POSITA, a person of ordinary skill in the art, would say yes, that's what I would do. Basically they would correlate information from all over the place, how do you send all the data to your SOC? You have to decide what to -- what to send. So negative, positive filtering is very natural thing to do. There are already things you don't care, because things normal. Keep the things that you think are likely to be attacked, further analyze it, correlate it, and then you're still not sure, using some analysis, which is, you know, at a time, at that time around late 1990, 2000, yeah, you basically use anomaly detection sentry as a last step of analysis meaning that you're not sure, air not sure it's attack or not. It's not exactly matching not attack what do you do you say using normal detection, you say at least it's not normal, then you say, hey, this is anomaly, at least you already selected something likely to be wrong, the volume is small enough, you send to SOC, that's what like I said, POSITA reading this description of sentry would agree,

basically it's captured by both Figure 1 and Figure 2, so.

Q So you said a lot there, I'm going to see if I understand it what your testimony is?

A Okay.

Q So you pointed to on 12 the description of the sentry filters. And those filters collect data using adaptive and proprietary sets of rules and then correlate data. Is it your testimony that based on that description on Page 12 of Exhibit 2009, it would have been the natural thing to do for a POSA to positively filter data, negatively filter data, and retain a residue?

MR. GOLDBERG: Objection to form. Of the mischaracterizes testimony.

A So like I said, you read sentry in the context of the whole MSM, right? It talks about SOCRATES as well, the SOC. And like I said, in my -- in my Paragraph 214, I talk about sentry collect data and give the volume of the, you know, basically using 20,000 filters as a lot of filters.

Then the next sentence says it you have then the sentry also utilizes an analysis engine to further analyze post-filtering residue, which is then sent to the SOC. And SOCRATES. So again, we talk about in the context of managed -- security monitoring. So the reason that you won't do this, there are certain things you're not sure you send to SOC but there are certain things you cannot send a ton of data, beginning when you send it over you should at least do some processing, like I said, any POSITA, certain of skill in the art would say, it comes in always normal, throw away, don't occupy my bank with and CPU, throw it away, that's negative filtering. That's obvious.

Then you sea, okay what's remaining, maybe then I can match, let's say for example, normal type patents match known attacks, known attacks are known bad things, then that's positive filtering then you block that traffic for example, then you say what's it meaning you're not sure but you already know, it's not known to be good not known to be good you you're not sure what to do,

like I said, in late 1990ss. In fact, my thesis was about exactly the same thing you put in anomaly detection to do further analysis for things that you're not sure. And that's exactly what he's talking about here. There is so much data from all over the place, it emphasized that the sentry goes beyond traditional ideas intrusion detection system. Okay.

And then it sends stuff to SOC, I mean a POSITA reading this would say, yeah, absolutely, that's exactly, like I said, architecture wise match Figure 1, on the left-hand side doing the customer side the sentry on the right-hand side you have SOC and SOCRATES and then further what does sentry do, first it does a POSITA would agree that's what Figure 2 is talking about.

Q So -- so if I'm understanding your testimony correctly, you're saying by the late '90s, you worked on this kind of thing that a POSA reading a description of using adaptive filters and proprietary rules in the context of an MSM would know that it would be obvious to do positive

filtering, negative filtering and retain a residue?

MR. GOLDBERG: Objection to form. Mischaracterizes testimony.

A So any POSITA, I think even before 1990s, there was so much traffic, you would throw away things that you know is normal, and try to focus on the remaining to say, can I see, I do see some known type patterns, awesome, block those, do whatever. And that was remaining, you can say okay, I've done my job, just give up, or -- but what Schneier and the patent talk about, no, no, wait, don't throw that away, do further analysis. That's called post-filtering analysis. The residue.

And then you say, how do you do that? You don't know for sure it's good, you don't know for sure it's bad, what the best you can do? I would say by -- I wouldn't say by 1990s I would say by mid '80s, people already talk about using anomaly detection to say okay you don't know for sure it's good, you don't know for sure it's bad, but at

least you can say, hey, is that anomalous. Like I say, any POSA would say, yeah, absolutely, of course, that's what you do.

Q Okay. Moving on to the last sentence in Paragraph 214, you say that, "trained security analysts work with the SOCRATES program to filter out the chaff and redefine the potential security threat information that is present -- presented to customers."

Do you see that?

A Yeah, I see the sentence, yes.

Q Is -- is that sentence trying to show that the Counterpane MSM meets element 1E of the '641 patent that requires a modification and control system for a dynamically modifying an analysis capability of the probe during operation thereof, based on the received feedback"?

MR. GOLDBERG: Objection to form.

A Can I have the reference 2012. All these things have been a while. And when I say I'm not familiar with the product features, I want to manage, I have not read the product or internal

documents. That's, you know, Exhibit 2009 is not internal documents. Okay. So (document review.)

Okay. So if you read the -- if you read the paragraph, the second paragraph on Page 2, right of Exhibit 2012 on Page 2, it talks about, you know, okay, I think I'd like to read let me see, maybe the third sentence, say, "refined event data is then displayed for customers on the secure web portal." I think that's example of 1D, receiving the feedback.

And then the next sentence say, "in other cases customers pay Counterpane to install and manage its firewalls and other security appliances and make changes to the servers to keep them safe." Right.

And then it say, "antivirus, antispam content control and protection from denial of service attacks or other options on its service manuals."

So I will say that the -- the sentence to say install and manage and make changes, that is example of 1E.

Q You said that, "make changes," that description is an example of 1E. But nothing in the text that you read from Exhibit 2012 talks about dynamically modifying an analysis capability of the probes, right?

A Just making changes. Again, say that has to be static.

Q Right. So it makes changes that could be either static or dynamic; is that fair?

A I mean, making changes, that's what is said. I mean, I have personal experience because I have a former student working in a similar company but not Counterpane. They do talk about how they make changes basically without shutting down customer service. -- they just send changes over to the customer side and will update the appliances on the customer side. And that's, I would say that's a much smaller company than Counterpane, so to me, like I said, POSA would say, yeah, making changes, it doesn't mean you have to do it only statically, it doesn't mean you have to restart your monitoring services or

mechanisms. Those things are there, so anyway.

Q So in the late '90s then, a POSA would read making changes and understand that that could include dynamically modifying the analysis capabilities?

A What I'm trying to say is that at least it's fine, as I know, like exactly what it says here, the customers can actually say, yes, I want dynamic updates, in fact this mode is called a search mode just give it to me, you don't have to verify, and then I have to go in there to explicitly download update, just update me whenever you feel like it, so that has been a well-known practice for a long time, I would say since the late 1990s, early 2000s. That's been a when I went to work in this company, late 1990s 2000s.

Q Your former student went to work for another company besides Counterpane, and you think that shows somehow that this description about Counterpane's product not just making changes means that Counterpane's product was dynamically

modified?

MR. GOLDBERG: Objection to form. Mischaracterizes testimony.

A What I'm trying to say is that that's a known art, that's a known art in particular.

Q As of what time frame, I'm just trying to clarify?

MR. GOLDBERG: No, no, are you withdrawing your question? Or let him answer.

MR. TUMINARO: No, I'm clarifying the question.

MR. GOLDBERG: You're withdrawing the prior question.

BY MR. TUMINARO:

Q It's a known art as of what time frame to do this dynamic modification?

A I would say by the late 1990s, early 2000, definitely. If you think about, you say okay, update, but just shut down your security monitoring system, then people gee what's going to happen. So my point is that for security monitoring, you want your system to constantly

working. You don't want to say okay, you know, to install the update, you have to shut down and restart. People say, no, I'd rather not do it. Because if you shut down and restart, that means there is a window of opportunity for an attacker to come in me so to me a POSA would agree that people who view this type of system, I teach this thing forever, almost 30 years now, you always -- when you deploy a security monitoring system, you constantly think about what the attacker would do to compromise your security system so that they can bypass your detection.

So you yourself, shutting it down just to get update would be the last thing you want to do, so obviously if you buy a product from let's say a company, buy a service from a company like Counterpane and say okay do update I do I have to restart, do I have to shut down, gee, if that answers yes I'm not going to buy your thing. That's common sense.

Q And that was common sense as of the late '90s?

A Yes.

MR. TUMINARO: Okay. We can take a break now.

MR. GOLDBERG: Yeah.

(Recess.)

Q Welcome back Dr. Lee.

Dr. Lee, Counterpane's MSM was not the only network monitoring service in the late '90s; is that right?

A Can you repeat that sentence again?

Q Counterpane's MSM was not the only network monitoring service in the late '90s; is that right?

A That's correct, yeah, they are not the only one.

Q And in fact Counterpane's MSM was not even the first network monitoring service; is that right?

A That I wasn't sure. I mean, I -- yeah, I mean again I didn't opine on that. I didn't look too deep into it, but, you know, managed security monitoring is something that people talk about in

starting a practice, but if they're first or second, I don't know, I don't remember.

Q And IBM had a network monitoring service before Counterpane; isn't that right?

MR. GOLDBERG: Objection to form. Scope.

A Which one you're referring to?

Q IBM had a net ranger, and along with net ranger it offered a service to have security analysts analyze traffic; is that right?

MR. GOLDBERG: Objection to form. Scope.

A I remember discussing, citing the petition expert's report when mentioning net ranger, but I can't recall how I talk about it.

Q Maybe I can try to help you out. I'll just hand you what was previously marked Exhibit 1037, a Book Titled Intrusion Detection by Terry Escamilla?

A Okay.

Q Have you seen this document before?

A I'm sure I've probably seen it, but I don't recall the details.

Q If you would turn with me to Page 276. Do

you see that there is a heading that says, "Which product has the best nose"? Do you see that?

A Okay. I saw the title, yes.

Q You see that?

A Mm-hmm.

Q I'll read it for the record: "An info world test recorded in the May 4, 1998, issue rated product -- products as follows, No. 1, IBM's outsource solution using NetRanger; No. 2, ISS Realsecure; No. 3, Network Flight Recorder; No. 4 AbirNet Session Wall."

Do you see that?

A Mm-hmm.

Q Do you agree with me that these are examples of remote monitoring services?

MR. GOLDBERG: Objection to scope. Form.

A What do you mean by remote monitoring services?

Q Well, I'm going to ask you that question. You previously offered a -- an opinion about the '641 patent, correct?

A Which -- which opinion?

Q I'll just hand it to you. You've been handed a copy of what was marked as Exhibit 2001 in IPR2019-01324. This is a declaration that you submitted in support of -- with respect to the '641 patent in that IPR proceeding; is that correct?

A Yes.

Q If you would turn with me to paragraph 60. Are you there?

A Yeah.

Q At the bottom of the last sentence in paragraph 60, it starts with, "remote monitoring services were known."

Do you see that?

A Hold on. 60. Hold on, Page 60, right?

Q No paragraph 60 is on Page 27?

A Okay. Sorry I confused the page -- okay all right. Remote okay.

Q The last sentence in paragraph 60, Page 27, you wrote, "remote monitoring services were known."

A Yes.

Q Is that a true statement?
A Yes.
MR. GOLDBERG: Objection to form.
Q What did you mean by remote monitoring services when you wrote that sentence?
A Let me look at that.
MR. GOLDBERG: I want to object. Outside the scope, and also form.
A (Document review.)
So this sentence I said remote monitoring services were known but not common, meaning it's not like every single SA intrusion detection network monitoring system provide remote monitoring, even though it's known, but I said here is not common. And also in particular there was no well-considered architecture to run them to help discover unknown intrusions.
And again, in sentence in the paragraph, in the context of paragraph 60, paragraph 60, I talk about managed security monitoring and say, you know, an a was a business in its infancy in 2000. Yeah.

So essentially I'm talking about, you know, remote monitoring service is in the context of managed security monitoring and then in paragraph 61 I talk about the 641 -- the '641 patent describes the entirety of novel architecture for remotely monitoring a network for intrusion. So -- and then talk about the Figure 1. So really what I'm trying to say is that I want when you ask, are they remotely, when I discuss -- this exhibit, are these remotely -- remote monitoring systems, I want to put it in context. So you gave me this opinion, then, yeah, then I would -- then now I know the -- now -- let's' agree when we talk about remote monitoring services we're talking about in the context of managed security monitoring.

Q Okay. And managed security monitoring services were known in the late '90s, right?

A So --

MR. GOLDBERG: Objection to form. Scope.

A Yeah, so I think late '90s, early 2000s, I mean I don't know -- I don't remember the exact

timestamp, you know, but again there is they're relatively new. There's some companies starting to pop up to do that, but, like I said, in my sentence here, paragraph 60 I talk about remote monitoring services were known but not common.

Q Okay. So looking back at Exhibit 1037 on Page 276, some of the companies that were listed include IBM. Do you see that on Page 276 of Exhibit 237?

A Yes.

Q And IBM offered a remote monitoring service, true?

MR. GOLDBERG: Objection. Form. Outside the scope.

A Again, I need to recall the details of the description of let's say net range or exactly what they talk about remote monitoring services.

Q Well, let's look at Page 276, 277, it talks about IBM and NetRanger. Do you see that heading?

A Okay.

Q Do you see the fourth paragraph under that

heading it says, "IBM's emerges response center.

Do you see that?

A Mm-hmm.

Q I'll read it for the record. "IBM's emergence response center offers a fee-based service with NetRanger. Instead of staffing your own team of security experts, you can use IBM's strength in this area. A network operations center is staffed seven by 24 and a specific expert is assigned to your account. When an event is detected, IBM's security experts notify you and help you respond to the event. Up front planning and response policy design also are available. As hackers become more sophisticated, outsourcing your network intrusion detection seems attractive because you may not be able to staff and maintain your own center of competency."

Do you see that?

A Yeah.

Q Is -- does this refresh your memory that the IBM offered security monitoring service?

MR. GOLDBERG: Objection. Outside the

scope.

Q In the late '90s?

A They -- they're offering secure monitoring and by the description here had nothing to do with architecture of Mr. Schneier's patent talks about. It basically talks about, hey, look, you got a product instead of you manage it, I'm remotely managing it for you. It doesn't talk about, hey, your local, your overall product that you deploy would do all these negative filtering, positive filtering, post-filtering analysis of -- of residues and then send it over to security center to do more analysis, and you know, so on. Talk about any of that, basically say, hey, I do it for you remotely how is it different from say I outsource my email to cloud provider now? That's how I see it. Nothing to do with Schneier patent.

Q So you would agree we me though that remote monitoring services would collect data from human analysts to analyze?

MR. GOLDBERG: Objection. Mischaracterizes testimony. Outside the scope.

A Can you repeat your question again?

Q This remote monitoring service offered by IBM would collect data for human analysts to analyze; do you agree with that?

MR. GOLDBERG: Same objections.

A That's not what it says here. Basically say -- when an event's detected they actually notify you, and that's what I said.

And also I think the most important thing is the second sentence. Instead of staffing your own team of security experts, you use -- you can use IBM's strength in this area, meaning that, hey, you're hands off, just buy my thing, I can remotely manage for you. That's very different from what Schneier is talking about, completely different I mean a POSITA would say, wow these two different things, what are you talking about? That's what why I keep asking you, what do you mean by remote monitoring.

Okay my opinion here is remote monitoring is in the context of managed security monitoring, which is not a common thing and architecture wise,

very -- there is no, not enough to know about it and that's why Schneier patent talks about hey here is architecture and IBM NetRanger had nothing to do with that.

Q Okay my question is not about Schneier's?

A Okay.

Q MSM, Counterpane system right now?

A Yeah.

Q What I'm asking about is the IBM system that's described here, we can also look at the real secure system that's described underneath. My question is: Let's start with IBM, IBM provided a service for human analysts to analyze data from a client's network; is that a fair statement?

MR. GOLDBERG: Objection. Outside the scope.

A Again, this paragraph doesn't state that. If just say, "when an event is detected, the expert would tell you.

Q Well, the human analyst would analyze data from a client's network; isn't that what this is

saying?

A No.

MR. GOLDBERG: Objection.

A That's not what it says. I can tell you a POSITA would tell you how -- how this service -- how this mechanism works. You put something there, you monitor.

Q Sorry --

A You have alerts, and then you look at the alerts, nothing -- because you look at alerts doesn't mean you analyze the data. That's a very different thing. This is different skills a POSITA would tell you, that's different skills. So what IBM is telling you here is that -- when an event is detected, security expert would notify you and help you respond to the event. It didn't say, oh, my -- my expert will go in there and locate your data, your traffic data no it didn't say none of that.

Q So --

A And like I said, a POSITA would tell you those are very different things.

Q So you're telling me that a POSITA think it's very -- when it's saying that instead of staffing your own team of security experts, you can rely on IBM's strength, you think that's not suggesting that IBM's security personnel could analyze data from a client's network?

MR. GOLDBERG: Objection. Mischaracterizes testimony. Outside the scope.

A But again, that's not what this paragraph is saying. All this paragraph is saying that a, you know, when an event is detected, IBM secure expert will notify you and help you respond. And that's actually exactly the job description of -- of security add my opinion, you locate the alerts and say, do I know this alert do I respond to it? What's my response? And that's very different from, oh, your job is look at the data and tell me what's going on. Look at the network traffic data, that's your job to analyze it and using all kind of scripts and programming write to do it, that's completely different jobs.

Q Maybe we're talking past each other. I'm

asking you not what the words say on the page. I think you're a person of ordinary skill in the art as of the time of these patents; is that right?

A I have my Ph.D. in intrusion detection, what do you think?

Q So?

A You're calling according to definition of POSITA, of course.

Q You are?

A Yeah, of course.

Q Because rhetorical questions don't really work very well in a deposition?

A Okay. That's fine.

Q So what I'm asking you now, as an at least a person of ordinary skill in the art, reading this when it says that rather than staffing your own experts, you can rely on IBM's strength in this area, is it your testimony as a POSA that that's not suggesting that the security experts at IBM would be analyzing data from a client's network?

MR. GOLDBERG: Objection. Outside the

scope.

A My testimony is this paragraph did not say so did not say what is described, only says the IBM security expert, when an event detected it would notify you and help you respond to the event. It didn't say the security expert would tell you, hey, I analyze data of this event happening. It didn't say so.

Q Let's look -- let's look at the -- the next product, Real Secure in Exhibit 1037. Do you see the heading that says real secure?

A Yes.

Q And I'll read it for the record, "ISS is already the market leader in scanning tools with safe suit. Real secure is widely used network IDS that complements ISS's other offerings. Like NetRanger, Real Secure supports remote sensing station called engines that report to a central console.

Do you see that?

A Yeah.

Q And you go to the last paragraph in that

section, it's on Page 279. It says, "ISS also relies on its X-Force team of security experts to find new attacks and create or adjust signatures."

Do you see that?

A Yes.

Q Doesn't that ISS was offering a service where human analysts could analyze data from a client's network to find new attacks and create or adjust signatures?

MR. GOLDBERG: Objection to form. Outside the scope.

A Let me -- let me look at the whole section. Okay? (Document review.)

Okay. So what's your question again?

Q The text on Page 279 related to the ISS Realsecure service, doesn't that suggest to a person of ordinary skill in the art that that service would collect and analyze data from a client's network to identify new attacks and create or adjust signatures?

MR. GOLDBERG: Objection to form. Outside the scope.

A Okay. So from what I read, that's not what this session talks about. It talks about sending a report to a -- to essential could you be but doesn't talk about how the analyst are using the console and what analysis they're doing on the report. That's point No. One.

Point No. Two would with regard X-Force which I happen to know them can talk about discovery can say come from the X-Force only research or from contacts that it has with the underground. You could highlight underground. So it didn't say that the updates, whatever they do is from customer data. It talk about own research and contacts from underground.

Q What are -- going back to 277, are these things called engines that are referred to as remote sensing stations. What do those things do?

MR. GOLDBERG: Objection. Scope. Form.

A So the so-called remote sensing station is a sense that you put on the customer side. That's remote with respect to the central side.

Q So that would collect data, data from the

client's network, right?

A Again, it didn't say it's customer data. Talk about, let me see --

Q Well, you just told me?

A It says report -- report to central console, look at console here, are they customer data? What data? I talk about network traffic payload? No. Basically just a bunch of events. That's what I see.

Q What I thought you told me I asked you the question what the engines do the remote sensing stations you say they're at the client's network; is that right?

A The remote sensing means the censors are remote, meaning the customer side. Customer is remote with respect to central.

And then I said they send the reports, not data, reports to the central console.

Q What it says is, "the real secure supports remote sensing stations," which you said are at the customer side?

A Yeah.

Q That report to?
A Yeah. Report, yes.
Q Report to?
MR. GOLDBERG: Wait --
Q It doesn't say send reports. It says, "report to central console"?
MR. GOLDBERG: Objection argumentative.
Q Isn't that true?
A Like I said, a POSITA would say, what does report to means. In particular I'm a big customer. Okay, I have a ton of data. Doesn't mean I send all the data over. Most likely not. There is a privacy security concern there all the time. I mean POSITA would say, are you crazy, I send all the data over. Most likely not, I send the reports, detect the events over, yeah, sure.
Q Is -- is this real secure an example of a remote monitoring service that was known in the late '90s?
MR. GOLDBERG: Objection. Scope. Form.
A It is remote monitoring, but like I said, it's not in the same vein as the Schneier patent

in terms of managed secure monitoring. I mean the late 1990s, yeah IBM ISS started 19 -- no, at the time still ISS, not IBM. 1996, yeah.

Q And the analysis capability of these remote monitoring services could be updated based on what the human analysts found, right?

MR. GOLDBERG: Objection. Outside the scope.

A I think I always said this, right, it talks about the X-Force -- so again, X-Force is, I know them too well, so anyway, in this context, X-Force a team of security experts, they will find new attacks, they will create or adjust signatures the second sentence of the last paragraph is most important, discoveries can come from the ex-force's own research and from contacts that it has with the underground. There's nothing to do with customers.

Q How -- how could the X-Force find new attacks without looking at the customer's data?

MR. GOLDBERG: Objection. Scope.

A I couldn't say this on record because they

talk about underground. They have a lot of ties with all kinds of agencies. I cannot tell you about. So my point is that here, clearly didn't say anything about customer. New attacks do you think new attacks always from specific customers, why do they have to have ties with underground, contacts with underground.

Q So they can use their ties from the underground to analyze the customer's data, right, you said you know these guys did they -- did they use the information from the underground to analyze clients' data?

MR. GOLDBERG: Objection. Outside the scope.

A So I don't want to say too much, okay but this paragraph did not say so. That's all I can tell you.

Q Well, the -- I know that you're reading the second sentence in the last paragraph on Page 279 where it says the discoveries can come from this other source, doesn't say they must come, right?

MR. GOLDBERG: Objection. Scope.
Q Is that true?
A Yeah, I would say can come, yes, sure.
Q And in the first sentence, it says that the X-Force team of security experts find the new attacks and create or adjust signatures. What are they -- what are they finding new attacks in?
MR. GOLDBERG: Objection. Scope asked and answered.
A This is exactly second sentence telling you -- telling you that's a known places to find new attacks.
Q What's the purpose a remote sensing engines that collect data if the X-Force team is not going to look at that data?
MR. GOLDBERG: Objection. Scope.
A Very similar argument to NetRanger. Some people just don't want to deal with it. They don't want to manage it, say, you manage it, I pay you, manage it. That's at least one motivation.
Q Yeah, so the customers don't want to manage their own data so they're sending it to

security experts, right?

MR. GOLDBERG: Objection. Mischaracterizes testimony.

A Again, I didn't say data, same argument, same answer I gave in NetRanger. You send the relevant information such as the detected events reports. I've not heard any company would send whole pack of data over to another company. That's like violating a bunch of rules.

Q Okay. Sorry, maybe we're talking past each other. I think maybe I understand now.

Maybe the raw data from the clients isn't sent to the security analysts, but information about the data that's collected is sent to the security analysts; is that fair?

MR. GOLDBERG: Objection to form. Outside the scope.

A So, again, that really depends on the partners and services. Some products just say send me the event or the event, whatever the number I can look it up myself locally because I already have the knowledge of what event talking

about, so again, you want to send the whole, how to put it, there are a lot of things to consider what data -- what report and what format, what content you send over. You want of course you want the remote center to basically help manage your system that's what remote sense something all about, but on the other hand you also want to worry about your own secure privacy.

Q Right I'm trying to break this down and sort of understand what's -- so whatever is sent from the remote sensing engine to the security analysts, it's enough to identify that a security event has occurred; is it that true?

MR. GOLDBERG: Objection. Outside the scope.

A Again, in general you want to send something that's useful to the remote -- remote center. That's, you know, a POSITA would agree with that and then POSITA would also agree that you want to worry about your own data security privacy and then exactly what format, you know, and frequency and all of that. That again really

depends on, you know, the product and service and agreement that you sign. So without, you know, reading a specific description I would not opine on it.

Q I'm not asking about the exact data that's sent, but what I'm trying to figure out is the remote sensing engines will collect data. Information about that data is then sent to security analysts and that information about that data that's sent to security analysts needs to at least be useful to the security analyst; is that true?

MR. GOLDBERG: Objection to form. Scope.

A So, again, sensor collects a ton of data. It don't send all the data over, an a firewall will actually tell you what are the connections coming in, so nothing to do with security, do you send the whole net flow log over, you shouldn't. So my point is that we can go back to the 641. It talks about sending information about the identified events. That's makes most sense. The data that's sent over has to be something to do

with security that you want the remote send -- remote sender to take a look, not just the random data that you collect, no you don't.

Q That's what I'm trying to understand, in the IBM NetRanger remote service or in the ISS remote service, they would collect data and then send information about that data to the security analyst so that the, at least the information that the security analyst get would be -- they would be able to discern whether there is a potential new attack or a threat; is that true?

MR. GOLDBERG: Objection. Form. Outside the scope.

A But again I keep saying that the information has to be about the identified event, not just say information about, you know -- cannot be information about whatever I collect, no, you don't, basically the point is that there is a purpose. You send data -- you send information over and that information is about the security events that's happening in your network, can be something that you want the remote sender to take

a look, for security purposes.

Q Okay.

A That's what IBM then talk about events detected by the sensor, then this IBM analyst would notify you, and same thing here, ISS talks nothing about sending a ton of data, you know, I think POSITA reading this would say reporting to central console, a POSITA would understand you report to whatever you detect is likely attacked or known attack, whatever, has to be security-related stuff.

Q I think I understand I just want to make sure, what is sent from the remote sensing agent in IBM or ISS, it's sent to the analyst but it's related to security?

A No, no, I didn't say analyst.

MR. GOLDBERG: Let him finish the question.

A Sorry. Yeah. I don't want to be misquoted. Go ahead sorry.

Q I missed what you said there because I was talking?

A I didn't say analyst. I always say remote -- remote sender, always say that, I never say analyst. I've never -- you can look at the transcript. Okay.

Q Okay. I'm just trying to understand your testimony. I'm not trying to put?

A Don't miss quote me. Don't misquote me any time you misquote me, I'm going to interrupt you.

MR. GOLDBERG: Wenke, let him ask the question and we'll object afterwards.

THE WITNESS: All right.

Q So in the NetRanger or in the ISS system, the NetRanger from IBM or the ISS Realsecure, data is collected from some -- the client side customer network, and then information about a security, potentially security event is sent to the security experts at -- at either IBM's outsource service or ISS outsource service; is that fair?

MR. GOLDBERG: Objection to form. Outside the scope.

A First of all, I mean, I never say send to

a security expert. I never ever said that. For net ranger and on Page 277, the fourth paragraph, wow, whatever, under the title of IBM NetRanger, it didn't talk about sending it to the security experts. It only talks about when an event is detected, the IBM security expert will notify you, and help you respond. I didn't say the event is sent straight to the expert. Never said so. So I'm not going to opine on that, but at least I didn't say that.

Likewise, in -- in ISS, it say in the first sentence -- well, whatever the -- the second sentence of whatever the last sentence of -- on Page 277, it says, "like NetRanger, Real Secure supports remote sensing stations called engines, then that report to central console, it never talk about sending anything specifically to an expert or analyst, so...

Q So in the IBM emergence response outsource service, how could the security experts that are described on Page 277 possibly notify and help respond to an event if those security analysts

never got information about that event?

MR. GOLDBERG: Objection. Scope.

A Again, those are information details. The point is that if it is so important that the report is sent to the expert analyst, specifically directly, whatever, it will be stated here, but it did not, so, nothing to opine on, but what it says is basically, a security expert will. When event is detected, when it says when an event is detected, IBM security expert notified you in how you respond to the event. Exactly how the expert know about the event, okay, we can ask IBM net engine.

Q You would agree with me that IBM's security analysts have to know about the event in order to help respond to that event; is that true?

MR. GOLDBERG: Objection. Scope.

A That's what it says. When it's detected, the expert also notify you. Now exactly how the expert know about it. There are multiple ways to do this. I mean, I'm not going to opine to it, unless you give me the IBM NetRanger's manual, I

can take a look, internal document.

Q Just as a matter of common sense, I'm asking for the IBM security expert to help respond to an event, they have to have information about that event, right?

MR. GOLDBERG: Objection. Scope. Asked and answered.

A Like I said, when the event detected, the security expert will respond. Okay. So they will know the event, yes, they will know the event.

Q In order for the IBM security expert to know the event, they have to be sent information about that event, right?

MR. GOLDBERG: Objection. Asked and answered. Scope.

A That's not true. I can tell you how the SOC operates. You go in the SOC, you can look at the monitor. Okay? And maybe, I mean -- again, this -- there are many ways to implement. You can implement and say, hey, the event pops up on the screen. You can take a look. It's like an event that somebody would take care of.

Q So if the event pops up on the screen, that's sending it to a security expert, no?
A No.
Q Why not?
A The SOC has a big monitor of everything. Everybody look at the same information. It's not specific to, hey, Nolan, or you, no.
MR. GOLDBERG: Object to scope.
A So, again, like I said, it's one example of way to implement this kind of system. I'm not again opining anything more unless you give me IBM Realsecure internal documents that say, exactly here's how we do it. Again, a POSITA would say, yeah, there are multiple ways to do this. I mean, again, it is so important that an expert or analyst personally would get a direct message, oh, event detected, that would be described here, since it's not, I will not opine on it.
Q Or it can be so obvious that you don't have to say it, because if a security expert is going to analyze data, they have to receive that data, right?

MR. GOLDBERG: Objection, argumentative. Are you testifying, Jonathan?

MR. TUMINARO: I'm asking a question. I asked the question.

MR. GOLDBERG: You're outside the scope and you're being argumentative.

A Hold on. So it's not -- it's not obvious. Like I said, if you know anything about network security monitoring, how the security admin works on SOC, there are many ways to do this, there are many ways things are being reported to the SOC people will take care of. That's the end of story, period. That's the only thing I will opine on it. The information sent to SOC, and like this paragraph is saying, when the event is detected, security expert will notify you and help you respond to it.

Q So like for Realsecure at the bottom of Page 277, it says that the remote sensing stations will send a report or information about an event to a central console.

Do we agree on that?

A Yeah, it says -- yeah, sends report to central console, on the top of 228, yes.

Q And the X-Force team of security experts could be sitting in front of that central console to get that information, right?

MR. GOLDBERG: Objection. Scope.

A Again, the only place it mentions X-Force is last paragraph. It not talk about console. It talks about underground instead.

Q What it says is, "The X-Force team of security experts will find new attacks and create or adjust signatures." To find the new attacks or adjust signatures, that must be based on information about the security event, no?

MR. GOLDBERG: Objection. Argumentative. Outside the scope.

A If that's the case, it will say so. But instead it said discoveries can come from the X-Force's own research and from contacts that it has to be underground. That's what it's emphasizing. Nothing to say -- didn't say anything about a central console, customer

information, none of that. So I'm not going to -- I'm not going to opine on that. You're being completely hypothetical.

Q These new attacks that are described in -- on Page 279, do you understand those new attacks to be at the -- on the customer's network?

MR. GOLDBERG: Objection. Outside the scope.

A Again, I didn't say so.

Q I'm asking you as a security expert, this is what you do, right, like you've been doing this for 30 years.

Where would the attacks occur?

MR. GOLDBERG: Objection. Outside the scope. Argumentative.

A Attacks can come from many places, but again, like I said, this paragraph -- paragraph talk when it talks about X-Force did not say anything about the remote -- the remote -- did not talk about the central console, did not talk about the report from the -- from a customer side.

Instead, it talks about its own research

and contacts with the underground. Why is it emphasizing on that? A POSITA would say, yes, that's the main source of information that they use to find new attacks and create new signatures. This is so obvious, any POSITA would agree with me.

Q So is it -- is this really what your testimony is today, that X-Force or IBM's teams were not analyzing customer data to figure out new attack vectors?

MR. GOLDBERG: Objection. Argumentative, mischaracterizes prior testimony, and outside the scope.

A So like I said, this paragraph did not say -- did not say X-Force analyzed customer data or using information on the remote counsel. It talks about X-Force doing its own research using the contacts with underground, and that's supporting the first sentence when it talks about finding new attacks and create or adjust signatures.

Q So I don't think that really answered my

question. What I'm asking you is: Is it your testimony here today as an expert in security that X-Force and IBM's teams were not analyzing information in customer's data to figure out new attack vectors?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony. Outside the scope.

A So, again, my opinion has to be based on documents, evidence presented in front of me. This is the only document I have. It didn't say anything about customer data. It didn't say anything about, you know, report from -- on the central console. So again, I can't opine, you know, on your question unless you give me some internal documents of ISS to say, hey, X-Force does X, Y, and Z and use customer data to do whatever. I mean without that, I'm not going to opine on that. Instead, I rely on the evidence, the document you want me to look at, which is here. It talks about discoveries can come from the X-Force own research and from contacts that it

has with the underground, and that's actually very much aligned with what I understand X-Force is about.

Q Okay.

A I can only say that much.

Q Okay. So I mean, I can read the document myself.

A Okay.

Q But you're an expert with, like, over 30 years of experience in network security. So I'm asking for, like, what your opinion is and what your testimony is, not necessarily what the document says.

A Mm-hmm.

Q So what I'm asking is: Is it your testimony, as you sit here today as an expert, that X-Force and IBM's teams were not analyzing information in customers' data to figure out and find new attack vectors?

MR. GOLDBERG: Objection. Argumentative. Asked and answered many times. Outside the scope.

A So, again, without documents about IBM ISS

and X-Force versus another team, I'm not opining on exactly which team is doing what. But this paragraph that you're citing is about X-Force. It did not talk about customer data. It did not talk about reports on the remote console. Is there any other team doing that on ISS? You give me document, I will opine on it. Otherwise, I'm not going to opine on it.

Q So based on what you know, did the IBM team and the X-Force team analyze information in customers' data to identify new attack vectors?

MR. GOLDBERG: Objection. Form. Outside the scope.

A Like I said, I can offer my opinion based on what's presented to me, which is here.

Q I guess I'm asking about based on what you know as an expert, not based on this information.

Based on what you know as you testify here under oath, did X-Force and IBM's teams analyze information in customers' data to identify attack vectors?

MR. GOLDBERG: Objection. Form.

Objection. Scope.

A Like I said, without reading the internal documents or charts and functions of different teams, I cannot comment on that, no.

Q So you don't have an opinion one way or the other? You don't know? I'm asking whether you know. I'm not asking about the documents.

MR. GOLDBERG: Objection.

BY MR. TUMINARO:

Q Do you know or not whether IBM and X-Force teams were analyzing information in customers' data to identify new attack vectors?

MR. GOLDBERG: Objection. Form. Outside the scope. Asked and answered. I think we're up to four times now.

A Like I said, I cannot opine on things that are not based on a written document that I rely on or you present to me.

Q So --

A If you produce a document, I can take a look to tell you, hey, what it says is true or not.

Q What I'm confused about is are you just not answering my question or do you not understand it? I'm not asking about what the document says. I'm asking about whether you know or not, and I haven't heard whether you know or not.

MR. GOLDBERG: Same objections. Now I think we're asked and answered five times.

MR. TUMINARO: But has he answered the question?

MR. GOLDBERG: He absolutely has.

MR. TUMINARO: Does he know? Do you know whether he knows?

MR. GOLDBERG: I'm not testifying.

MR. BLOCK: You said he's answered.

MR. GOLDBERG: He absolutely has answered. And you're not taking the deposition, so I ask that you remain quiet.

A So like I said, I'm going to opine on the documents in front of me, I cannot based on, well, I mean, yeah, like I said, there could or could not be -- again, like I said, if X-Force doing it, they would tell you X-Force doing it, but it

didn't say X-Force doing it.

Is any other team doing it? Well like I said, I need to look at some documents regarding how -- how ISS was organized at that time, you know, in whatever the time frame is, right, and who is doing what, and -- and, I mean, otherwise, I may be offering opinion that's not accurate enough. I'm not going to do that.

Q Are you offer -- the opinions that you express in your declaration, are they based solely on the documents we read or are you also relying on your expertise as a person who has worked in this field for, like, 30 years, in network security?

A Like I said, you know, I offer my opinion in my report based on evidence and proofs from documents that I cited and, of course, I would use POSITA to say yes, but I think this POSITA would agree, you know, my opinion, yeah.

Q So in offering the opinions that you express in your declaration, you are relying on your own personal knowledge and expertise in

network security; is that right?

A Again, we -- if it will go to specific opinion I offer to answer that question. The point is if something specific, let's say IBM ISS -- sorry -- ISS X-Force, that's a specific question. I want specific document evidence for that. If I say in general, what data did you send over, I will answer that question, in general how did we look at, I will answer that question, if you say exactly what --

Exactly what NetRanger is doing, exactly what ISS is doing. I need to look at their document to be specific to your specific question. That's what I'm trying to say.

Q So then I'll make it in general --

A Okay.

Q -- in remote monitoring services, data is collected at a remote site and the analyst or the security experts who look at the information -- the security experts, in order to find attack signatures in that client network, they're looking at information collected from the data on that

client's network; is that true?

MR. GOLDBERG: Objection. Form. Outside the scope.

A So, again, a POSITA would tell you that at the security center this whole chain, whole workflow, whole chain of information, okay. So who is doing what, like I said, that's very organizational-specific. Each company works in different ways. I would say X-Force is probably far end. The customer data, let's say is here. By the time it gets to X-Force, probably it's over there. So that's why I say, I need to look at the org chart and different teams doing what to tell you what they are doing.

So, again, like I said, the information is sent over. The report is sent over to the -- to the security operations center or central console and then exactly what process is use to -- to handle the data -- again, that's very specific to organization. So I cannot comment on questions such as, here's what ISS is doing, here what NetRanger is doing. I need to look at the

documents.

Q I appreciate that. I understand what you're saying. I'm not trying to ask about ISS or IBM.

A Okay.

Q I think what I heard you say -- I'm not trying to put words in your mouth, but correct me if I'm wrong, I think what I heard you say is that if a report is sent over to a security expert --

A Again, I never said security expert. Again, I keep correcting you. Don't put words in my mouth.

Q I thought those were the words you used --

A I said central console. I said sent to the remote central console or SOC, and then the data would be processed in some way.

Q Okay.

A I never said the report sent to the security expert or analyst. You keep trying to insert into my testimony, which I completely object.

Q Sir, with all due respect, those are the

words I hear you say. I don't have the realtime in front of me.

A Okay.

Q I'm just trying to use the words I heard you say, with all due respect.

A I'll keep correcting you.

Q I'm not trying to offend you.

A I will keep correcting you every time you say that.

MR. GOLDBERG: Wenke, we're going to blow out the court reporter, so let's give courtesy with her.

Q I think you said, correct me if I'm wrong, that a report is sent over to a central console; is that right?

A In the --

MR. GOLDBERG: Objection to form.

A -- case of ISS.

Q So I didn't want to ask you about a specific implementation because you object to that. So I wanted to ask you about in general for remote monitoring services, okay?

A I also used -- say SOC, secure operation centers.

Q Okay.

A Okay. That's fine.

Q So a report is sent over -- how about for analysis, somewhere?

MR. GOLDBERG: Objection to form.

BY MR. TUMINARO:

Q Are we on the same page at least?

A Sent to, let's say, a central console or secure operation center, yeah.

Q Okay. That report would include information about an event at a client's network; is that fair?

MR. GOLDBERG: Objection to form. Scope.

A I already said -- you know, basically, if you read the -- 1C of -- of Schneier, it talks about information about the identified events. I mean, that's a definition I want to use, meaning the information has to be about some security events or suspected security events. It can't just be anything. Because SOC means security

operations center. Security is the keyword. You don't send random junk. You send security-related events, information, over.

Q Okay. So data is collected from a client's network, put into a report somehow. That report is sent to a secure operations center when you're talking about a remote monitoring service; is that fair?

MR. GOLDBERG: Objection to form. Are we talking about any specific system or just some generic system?

MR. TUMINARO: No. Just in general because he wanted to talk in general about how -- he said remote monitoring services were known. He didn't want to talk about a specific service. So I wanted to talk in general --

MR. GOLDBERG: Okay.

MR. TUMINARO: -- how this happens.

A Hold on, so when you say I wanted to talk about general, that's how we started. We say if you want to ask me questions about ISS or NetRanger, I want to look at a specific document

of NetRanger and ISS. And that's when you -- when you want to say, let's talk about general, okay. I didn't initiate that. So put it in the record.

Second thing is I want to use '641 as a context. That's why we are here. Okay. So when you say the remote sensing systems collect data and then send over, no, you read the -- read the limitation here, which is a reflection of the architecture that we talk about for manage -- manage security monitoring is that you do all this in a filtering, post-filtering analysis, and send -- basically analyze the post-filtering residue. You don't just collect data and send the report. No, you do some analysis of the report and you send what you concluded as security event and send the information related to the -- identified events over. So a lot of work done on the remote side before send anything over. That you gloss over.

Q For ISS there is a central console, right?

MR. GOLDBERG: Objection. Scope.

A It talks about, yes, sending engine's

report to central console.

Q Where would that central console be located?

MR. GOLDBERG: Objection. Scope.

A It didn't say. It's not important. It's basically all you care about, one is central, one is remote.

Q Well, the central console would not be at the client, right?

MR. GOLDBERG: Objection. Scope.

A I would -- I wouldn't rule that completely out, no. I wouldn't.

Q What does it mean to be remote then?

MR. GOLDBERG: Objection. Scope.

A Remote is respect to central. You are here, he's remote. That's -- that's the -- that's the common sense.

Q Okay. So the central console is not at the same location as the engines; is that right?

MR. GOLDBERG: Objection. Scope. Mischaracterizes prior testimony.

A So, again, all these things are relatives.

Q Yeah, that it's relative. They're not at the same location. The central console is not at the same location as the --

A No.

Q -- remote engine.

A Okay. So what's a location?

MR. GOLDBERG: Same objection, asked and answered.

A You can be in the same -- New York City or same company, whatever, side, next building, next room. I mean just, yeah, in computer terms remote and central is completely relative.

Q So ISS has a central console, right?

MR. GOLDBERG: Objection. Scope.

A What do you mean?

Q The words that the Realsecure reports remote central stations that report to a central console, right?

A Yeah, it talks about 2A, central console. It doesn't mean it's total -- ISS only has one central console. It's very different concept.

Q So ISS has a central console?

A With respect to these remote sensing engines. It doesn't mean that it cannot have multiple central consoles somewhere depending on customers. It didn't say anything like that, you know, so anyway, just you have to read whatever is being --

Q Does.

A -- written.

MR. GOLDBERG: I'll object on scope.

BY MR. TUMINARO:

Q Does anyone look at that central console?

MR. GOLDBERG: Objection. Scope. Form.

A I mean, I would say that based on the description here, yeah, the -- the reports on the central console can be looked at. Let's put it that way.

MR. GOLDBERG: Jonathan, we've been going about an hour, when you find a convenient spot for a break.

MR. TUMINARO: Can just ask a few more questions?

MR. GOLDBERG: At a convenient spot.

That's I'm saying, about an hour.

MR. TUMINARO: Thank you.

BY MR. TUMINARO:

Q Then on Page 278, the last paragraph, do you see that it says, "Once activated, the console begins receiving data from the remote engines"?

MR. GOLDBERG: Objection. Scope.

A Yeah.

Q Do you see that?

A Yes.

Q "You could choose from a number of different views on the console, including by node or by event severity."

Do you see that?

A Mm-hmm.

Q "Data from the engines is logged and a variety of reports are possible."

Do you see that?

A Yes.

Q When it says "event severity," is that referring to like a security-related event, potentially?

MR. GOLDBERG: Objection. Scope.

A Yeah, potentially. I mean, again, you know, yeah.

Q And that the identification of that potentially security-related event was based on data that was collected from the remote engines; is that fair?

MR. GOLDBERG: Objection. Scope.

A It's not clear. I mean, it could be that when they report over, they already have a -- have some kind of a rating. I don't know. I mean, it didn't say that you analyze data and then rate them and then order them. No, it didn't say it that way.

Q But it does say you begin receiving data from the remote consoles, right?

MR. GOLDBERG: Objection. Scope.

A It says so and when you view them, you can order them by event severity. It didn't say they first analyzed it, rate them, and then -- and then -- and then ordered them. No, it didn't say so.

It just said, yeah, based on the data you can essentially sort them based on event severity. So -- so they didn't say anything about you analyze the data or report from the remote engine to -- to assess the event severity. It didn't say anything like that.

Q In order to determine the event severity, the data would have to be analyzed, no?

MR. GOLDBERG: Objection. Scope.

A So that sort of thing is what I'm trying to say here, is that it didn't say the data from the remote engine is analyzed at the console in order for it to rank them by event severity. What I'm trying to say is it didn't say anything like that. So I cannot say, yes, the data has to be ranked -- analyzed and then ranked by the remote console in order to order them based on the event severity. It didn't say anything like that, so I cannot draw the conclusion. I don't opine on that.

MR. TUMINARO: Maybe we should take a break now.

(Recess.)
BY MR. TUMINARO:
Q Welcome back, Dr. Lee.
I'd like to turn to the '641 patent.
A Okay.
Q And look at the claims.
A Okay.
Q And element 1B refers to a filtering subsystem; is that right?
A Yes.
Q Did the inventors of the '641 patent invent the concept of filtering?
A Filtering in what sense?
Q I guess I'll ask you what does filtering entail?
MR. GOLDBERG: Objection to form.
A In what context? Is it in security monitoring context or what context?
Q Yeah, in security monitoring context, what does filtering entail?
MR. GOLDBERG: Objection to form.
A Again, can mean many things in

different -- different instances. I would say in 1B talks about, you know, the "filtering system analyze status data to identify potentially security-related events represented in the status data, wherein the analysis including -- that includes filtering followed by analysis of post-filtering residue -- post-filtering residue is data neither discarded nor selected by filtering."

So that's the context of '641, but if you ask in general what filtering mean, again, it really depends on what data you're talking about, what goal you want to accomplish, so.

Q Would an "if statement" be a filter?

A Say again.

Q An "if statement"?

MR. GOLDBERG: Objection. Form. Scope.

A Again, depending what if statement you're talking about. Give me, yeah, I have to basically opine on, you give me -- how you put it? You give me specific example, then I can opine on the specific example.

Q What does the '641 teach about how filtering is performed?

A I think that's what it says in the 1B.

Q Does the '641 describe what positive filtering entails?

A We can go to -- yeah, I think we can -- let me see, yeah. It talks about, I think in -- let me see here.

Yeah, so if you read the Column 8, paragraph -- sorry, Column 8, Line 51 of the Schneier patent, it talks about "once collected, the data is first filtered by negative filtering subsystem which discards uninteresting information and then by positive filtering subsystem, which selects possibly interesting information and forwards it -- you know, and so on. So that's -- here you go, that's positive filtering.

Q Does the '641 patent describe how to implement a positive filtering subsystem?

A Let me look at is there any specific examples? Report --

So, okay. So I do not find specific

examples. Looking for specific examples that they offer in terms of positive filtering, but I would say I think in the report -- I mean, the patent talks about the kind of information being sent over to SOCRATES. They actually give you some insights in terms of what are the -- what kind of information related to identified events being sent over. But like I said, POSITA looking at the definition or description here, like I said, Column 8, you know, the sentence starting Line 51, yeah, we understand, yeah, positive filtering means things that are possibly interesting information. So there are many ways to do this. A POSITA would know how to do it.

Q So does the '641 patent in the -- describe how the positive filtering subsystem actually selects the interesting -- potentially interesting information?

A So you -- I would refer you to a -- figure -- Figure 2, right? I mean Figure 2 talks about where the information is coming from, from a bunch of sensors. Then you look at the status

data from the sensor to negative filter, meaning they throw away things that -- discard things that are not interesting, and then identify things that are likely to be interesting. And like I said, POSITA would read that and say, yeah, it makes a lot of sense. I mean, POSITA would say, yeah bingo, I can do X, Y, and Z, depending on my particular network.

And I think that's -- the patent also talks about the kind of sensors. It talks about -- let me see here. I think there is a place that talks about examples of these sensors. Yeah, for example, Column 5, starting -- the whole paragraph starting Line 4 talks about different kind of, you know, sensor status data you will look at. So like I said, POSITA reading this and also understand the context of -- of Figure 2 would say, okay, yeah, if you want to identify things that are interesting, yeah. I mean, here is kind of -- here are kind of things that we can do, so... I mean, yeah. That's a -- like I said, POSITA would know.

Q And I don't want to -- I'm just going to quote what you said. It said -- the sentence starting at Line 51 in Column 8, "will understand you have positive filtering means that things are possibly interesting information. So there are many ways to do this, a POSA would know how to do it."

A Mm-hmm.

Q So a POSA would know how to implement a positive filtering because it was known at the time of the '641 patent how to do positive filtering, right?

A As defined by '641, yes, you identify things that are interesting. That's the job of secure monitoring, anyway. So a POSA would know, yes, that's part of the job to implement the system, but exactly what filters, again, depends on the product that you're implementing, the kind of customer you are servicing and so on, but the principle and technology behind it is well-known.

Q So the inventors of the '641 patent didn't invent the basic concept of positive filtering; is

that right.

A I do not know whether the term positive filtering is something that he uses, but like I said -- like I said in my -- earlier, like I said, if a POSA reading the patent would, say, oh, by positive filtering we know how to do this. Now some of the people may use some other term that's not positive filtering. You can't just be looking for patterns of possible attacks. That's something that, like I said, if I read column A starting 51, I don't know, looking at positive filtering means select possibly interesting information. That's exactly what POSA will know. Of course, that's what we do, whether they call it positive filtering or not, that's besides the point.

Q Without using the term positive filtering?

A Right.

Q Or negative filtering?

A Right.

Q The inventors of the '641 patent didn't invent the concept of filtering to select

potentially interesting information.

That was known, right?

A Like I said, I would say that the inventor when he meant filtering, he meant what 1B was talking about. And if you say in general the security monitoring -- security monitoring or security filtering is something that is well understood, people say in general, yes, but exactly what it means specifically, again, it really depends on the product you're talking about, the kind of data you are going to handle, and so on and so forth. So like I said, general concept is, like, the security monitoring known, yes, in general, but exactly how they do it depends on context.

So filtering, the same thing. Generally, yes, a known concept, in general. But specifically 1B is 1B.

Q Okay. And, in general, the concept of filtering to discard uninteresting information was generally known; it's not something that the inventors of the '641 patent invented?

A So in general, I would say -- so, again, you know, like I said, first of all, 1B talks about both negative filtering and positive filtering and then looking at the post-filtering residue, I think that's new in terms of post-filtering residue, but in terms of, let's say, isolate to say is negative filtering and positive filtering, no. I mean if you -- like I said, if you read the column A starting on Line 51, people will say, yeah, I understand what -- what the patent is talking about.

If you ask POSITA, hey, can you implement that, most of them say, yes, I can implement that and exactly how you implement, then the answer would be give me the spec of the product -- give me the specification of the product you want me to build, then I'll build it specifically for that, but a concept in terms of negative filtering means -- means discarding uninteresting -- uninteresting information, or positive filtering which means select possibly interesting information. Those are in general well-known

concept to POSA.

Q What does the '641 patent describe with respect to how to generate the residue?

A What do you mean by generate?

Q Well, you read the portion that at Column 8, Line 55, "Data neither discarded by negative filtering subsystem, 220, nor selected out as interesting by positive filtering subsystem, 230, form the residue, which is sent to the anomaly engine, 250, for further analysis"; is that right?

A That's what it says, yeah, it says form the residue.

Q So does the '641 patent teach a POSA how to form the residue?

A So the '641 patent talks about data that's neither discarded by negative filtering nor selected as interesting by positive filtering subsystem form the residue, F-O-R-M, form the residue. So that's a teaching.

Q So how would a person of ordinary skill in the art know how to implement a system in order to

form a residue --

MR. GOLDBERG: Objection.

BY MR. TUMINARO:

Q -- based on what's disclosed in the '641 patent?

A So a POSA reading this will find it so obvious. Data comes in, negative filtering, throw everything that's not interesting. Positive, meaning positive -- go to positive filtering, select things that are, you know, likely interesting. Whatever is then -- whatever is remain there goes to -- that's -- that forms the residue. I mean that's a teaching. So obvious.

Q The inventors of the '641 patent didn't invent the concept of positive filtering and negative filtering and forming a residue; isn't that right?

MR. GOLDBERG: Objection to form.

A That's not what I said. I said in the context -- okay. Hold on. So basic '641 talks about filtering and 1B talks about filtering. And that's new because it talks about post-filtering

residue, and you perform more analysis on the post-filtering residue. That was new.

Q Yeah, so I guess I'm not talking about the analysis on the post-filtering residue. I'm talking about how to form the residue. And all that the '641 patent says is you do negative filtering, positive filtering, and you form the residue.

How would a person of ordinary skill in the art know how to implement a system that does that?

A Okay. So like I said, in Column 5 -- sorry, Column 8, Line 55, talks about "data neither discarded by negative filtering subsystem, 2020, nor selected out as interesting by positive filtering subsystem, 2030, form the residue. That's as clear as you possibly can be to any POSA. Data comes in, negative, positive, residue. What else do they need to be taught?

Q Well, how would a POSA know how to identify something that's interesting in the data to be positively filtered?

MR. GOLDBERG: Objection to form.

A I think I answered the question when you asked what positive filtering means. I referred to -- you to '641 patent, Column A, starting Line 51, right, positive filtering means select possibly interesting information. And POSITA would say, yes, that's what secure monitoring system will do, figure out -- try to select what's likely to be interesting for security purpose, analysis purpose. That's exactly the point of doing part of job -- that's part of the job of doing security monitoring, so. Yeah, I mean, like I said, POSA would completely agree with me that they know how to do this by reading the patent.

Q Okay. How would a POSA know how to identify or discard information that's uninteresting?

MR. GOLDBERG: Objection to form.

A Can you repeat the question again?

Q How would a POSA know how to discard uninteresting information?

A Again, it's multiple -- so, again, there

is a concept that's very basic, a POSA would already know, and then by reading the patent, oh, by negative filtering you mean something that's not interesting, you discard them. And a POSA would say, of course, I just ignore them. I just let it go, decide if you would -- which connection coming in. It's not interesting, to let go. Don't do anything.

That's -- it's basically from analysis of filtering point of view that you're discarding it from the analysis point of view. I mean, that's -- a POSA would know that.

Q So I think what you're saying is a natural consequence of the negative filtering and the positive filtering would be a residue?

MR. GOLDBERG: Objection to form. Misstates prior testimony.

A So, again, like I said, if you read Column A, Line 55, it says, "data neither discarded by negative filtering subsystem, 2020, nor selected out as interesting by positive filtering subsystem, 2030, form the residue."

Yeah, that's as clear as it is stated.

Q I can read it, but a natural consequence of negative filtering and positive filtering is a residue; is that what your testimony is?

MR. GOLDBERG: Objection. Form. Mischaracterizes the prior testimony. Argumentative.

A Like I said, I rely on the statement here, "data neither discarded by negative filtering nor selected by positive filtering form the residue." That's the definition of residue.

Q I'm not asking about the definition of the residue. I'm asking whether the residue is a natural consequence of positive filtering and negative filter.

MR. GOLDBERG: Objection to form. Asked and answered.

A I already answered the -- what residue is. Data neither discarded nor selected form the residue.

Q And I'm asking you whether the residue is a natural consequence of negative filtering and

positive filtering?

MR. GOLDBERG: Same objections.

A So I don't understand what you talk about natural consequence, if I already gave you clear definition of what is residue. It's like I said, a POSA reading this would say, yeah, I understand what residue is. I know exactly how to implement this. That's all I can say. It's as clear as stated.

Q Okay. And a POSA would understand how to implement that because the concept of selecting out information that's interesting out of data, discarding information that's disinteresting out of data and having a residue, that was a known concept, right?

MR. GOLDBERG: Objection to form.

A Like I said, multiple times, 1B, Claim 1B, is new.

Q Yeah --

A So like I said, people understand the concept negative filtering according to -- to description of the patent. People understand the

concept of positive filtering according to patent, but how -- what to do with the residue is something new. And that's exactly what the patent is about in 1B.

Q So maybe I'm not being clear. I'm not asking about 1B right now. So I'm not asking about that.

A Okay.

Q I'm asking about the -- the concept of positive filtering, negative filtering, and having a residue left over, that concept was known before the inventors of the '641 patent submitted their patent, right?

A I -- I don't recall seeing people talk about residue, to be honest, okay? So like I said, there is a reason that 1B is novel. It talks about, hey, a specific points out there is a post-filtering residue that requires more analysis. So my point is, if that's a known thing, then, like I said, point me to something that talks about residue, point me to something that talks about post analysis of residue, then I

can opine on. I haven't seen anything on that.

Q I'm trying not to get hung up on the words. I'm not talking about the words. I'm talking about the concept. You said the concept of, sort of, positive filtering was known?

A Yeah.

Q The concept of negative filtering was known.

A Mm-hmm.

Q And I'm asking about the concept if you do negative filtering, then positive filtering, the concept of data being left over, whether it's called a residue or not, that concept was known; is that true?

A Like I said, I can't recall any discussion, description, invention of that nature. That's all I can say.

Yeah, there are all these things left over. What do you do with it? That's why Schneier talks about it.

Q I'm not asking about -- talking about what to do with the stuff that's left over. I'm

talking about the concept of --

A If people don't talk about that, that means there is no concept that I can recall.

MR. GOLDBERG: You -- Wenke, you got to let him ask his question.

THE WITNESS: Okay. Sorry.

Q Maybe people didn't do anything with the leftover data. You don't recall seeing anything about people doing stuff with the leftover data, but the concept of negative filtering and then positive filtering and having something left over, that concept wasn't invented by the inventors of the '641 patent?

MR. GOLDBERG: Objection. Asked and answered.

A So like I said, I don't recall any references that talks about the leftover data in any meaningful way that register in my memory, no, I have not.

Q What -- what about the Chu reference, that's a reference you looked at that's in this proceeding, right?

A Yes, I looked at Chu reference.

Q The concept of having a white list and a black list and having something that satisfies neither; that was known, right?

A Okay. So let me see -- yeah, so in my report, I think on Page 11 I talk about this one example. I think there is only one example in the whole thesis talks about white listing, black listing, and then it's unknown.

Q So you would agree with me that the concept of positive filtering was known. The concept of negative filtering was known before the '641 patent, and the concept of having something left over after those two types of filtering was also known, right?

MR. GOLDBERG: Objection. Asked and answered. Form.

A So as I said, you know, a POSA would say, yeah, there are always things left over. I think the key is what do you do with it? And I would just supplement what I said earlier that in a security monitoring setting, I don't recall sort

of papers and documents talk about specifically what do you do with the -- whatever left over unknown or residue, what do you do with that to improve your security monitoring -- I mean, that's something I've not seen or registered in my memory. That's why I say '641 is novel that way, at least 1B. That's -- the 1B is talking about that. So yeah, so Chu is completely something else, not in a security monitoring domain, that I know.

Q Before the '641 patent, databases were known, right?

A Database in what context?

Q Databases were known?

A Yeah, database, people use database since the '70s, I think, '60s maybe.

Q And it was known that databases could be updated either offline or dynamically, right?

MR. GOLDBERG: Objection to form.

A I don't specifically recall database being updated dynamically or -- I think most of the time -- it depends on what database talking about,

right, database on permanent storage, meaning the hard drive, kind of, yeah, in the persistent storage, that means in the hard drive, that you normally do it statically.

Q Well, you've heard of Microsoft database?

A Which one?

Q How about MySQL?

A Is MySQL a Microsoft database, I'm not sure.

Q How about SQL server?

A Okay. SQL server is different from database, but just server, okay.

Q Is -- SQL server is not a database?

A A server is server. Database normally would refer to the system that manage the database, and server would be, I don't know, handling remote inquiries, but anyway, yeah, those are.

Q Have you heard of Oracle database?

A Yes.

Q Are you heard of MySQL database?

A I've heard of it, but not very familiar.

Q In the '90s, would the SQL server database be updated while it's still online?

A I don't recall seeing that. I mean, I do recall research trying to basically synchronize the system, you know, while running with the updated databases very, very, very, very -- how to put it -- resource intensive kind of work. So I just do not know for a fact that was the industry practice.

Q The Oracle database in the '90s, could that be updated while it was still online?

A I don't know any -- any document that says so, no, I cannot opine on that.

Q You don't know any document, one way or the other, that says it can't be or it can be update -- the oracle database can be updated online?

MR. GOLDBERG: Objection to form.

A So, again, depending on what database talking about, are you talking about database in storage, which database is being currently used in transaction? So the latter means that data

probably already has in memory the software is using. So how does that correlate the data you're using right now in realtime versus data being updated in the storage. That's a lot of synchronization. That's super hard.

You can update the permanent storage that's on drive, but then the data that you're using is out of sync with the other one. You say, oh, I'm going to update the one that you actually, in memory, that's very, very hard to not to screw up system, because it's going to screw up -- because you cannot just go into memory and flip the script without crashing the database system. Then, again, even you update in memory copy how these things -- again, even if you can update in memory copy of the data, how do you synchronize with the update you want to do in the permanent storage. There is a ton of research going in. That's to the extent I know, that is super hard problem is not obvious that anybody is practicing it in practice unless you show me a document.

Q So is it your testimony, as you sit here

right now today, that the Oracle database in the '90s was not able to update data while it was online?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony. Asked and answered.

A So like I said, I would love to see a document that tells under what condition, at what cost, and so on, so forth, that you can do that. Without it I cannot opine.

Q So you -- is it your testimony that you don't know, one way or the other, as you sit here right now, whether the commercially available databases in the '90s could update the data while it was online?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony.

A So like I said multiple times, it really depends on the situation exactly what they mean by database. Is database in storage, was database in memory that's being used? Which one are you talking about when you do a dynamic update, okay?

And then exactly how do you do the update, what technology, what cost you're doing it, and then how do you make sure that the data that you're using right now in realtime is synchronized with the data on your hard drive. Again a lot of details I cannot opine, say, hey, is Oracle doing this or not. Give me a document, I can opine on it.

Q What I'm asking you is, as you sit here right now, whether you know whether the commercially available databases at the time, like SQL Server or Oracle Database or MySQL, whether they had the ability to update data while those databases were online? Do you know the answer or not?

MR. GOLDBERG: Objection to form. Asked and answered.

A Like I said, I know a lot of there was a lot of research going in. I know a lot of the factors to consider is a super hard problem. So like I said, I would love to look at industry reports, product documents description. To opine

otherwise, I will not an opine on it.

Q Can you give me an example of a commercially available database in the '90s that did not have the capability of being able to be updated while online?

A So I think I already answered the question, right? It really depends on what situation talking about, you know, like what data you're talking about, what database you're talking about. Is the permanent storage, you know, the database in permanent storage versus the database that's already loaded in memory, and how big is the operation, how large is the data set, what's the realtime requirements, what do you mean by dynamic versus can you, like, pause and update and then restore. I mean there are a lot of details going into the systems, because systems work in computer science, basically, they would say the devil is in the details. I cannot comment on those, the details, without reading the documents. The devil is in the details without reading the document.

Q I understand there are a lot of different situations and scenarios that you're talking about.

A Mm-hmm.

Q But I'm asking whether you can identify a single example of a commercially available database in the '90s, in any situation, in any configuration, where that database could not be updated while still online?

A Sitting here right now, like I said, I need to read more documents or product description at that time to opine on that. Otherwise, like I said, I would not able to render my opinion. I just tell you that this is super hard problem, not well defined. Everybody has their own idea of what's database, which database they're talking about, what do they mean by dynamic versus not, and so on, so forth. Again, I'm not going to opine on that.

Q Have you ever heard of such a commercially available database in the work that you do that did not have the capability of being updated while

online?

A Personally, for all databases are used, none of them I rely on dynamic updates.

Q I'm not asking whether you rely on them for dynamic updates. I'm asking whether you know of any databases from the '90s that did not have the capability of being updated while online?

A So I think I answered this question multiple times. I -- I'm not aware of any database that -- is able to do dynamic updates. I'm not experienced. I have not heard of.

Q And which databases do you use?

MR. GOLDBERG: Objection to form.

A Right now, I mean, I am familiar with Oracle, you know, Postgres, Ingres, that kind of thing, MongoDB, whatever, yeah.

Q And the Oracle database that you're familiar with, can you insert data while it's still online?

A So, again, like I said, it really depends on a lot of situations. I mean, meaning that each application they are running rely on that data,

right? So like I said, updating the database mean many different things, meaning the update by default permanent storage, then do you have a copy of the data in memory.

Then how to sync the update in memory, but you say, oh, I'm looking at different table, I don't know if that table you're updating. Okay, then you do have a synchronization problem.

Again, a lot of these details, when people talk about, oh, I can update, I really have to look at dynamic update. I need to look at the context to say, hey, I can detect -- I can detect -- you do security monitoring, you say, I can catch, you know, all these attacks. Normally, they have to -- they have to qualify in what context, what scope. Same thing here, if you ask me this database can be dynamically updated, I'm going to ask you all these questions in what context, what scope? Without that, I cannot opine.

Q I guess --

A It's very complex problem. That's what

I'm saying.

Q I guess I'm not asking for your opinion and I'm not asking for a lot of detail. I'm asking, in your experience in the Oracle database that you are familiar with that you used, can you insert data while it's still online?

MR. GOLDBERG: Objection. Form. Asked and answered.

A Like I said, I'm not aware of doing that. I'm also not aware of other people doing that. You know, again, like I said, updating database, the scope can be very broad. The problem is so complex. So I'd rather have a very specific scenario to opine.

Q So is your testimony, as you sit here right now, you're not aware of anyone who has used an Oracle database and inserted data while the database was online?

MR. GOLDBERG: Objection. Form. Mischaracterizes prior testimony.

A I think I said this multiple times. This problem is so complex, the scope can be so wide,

you cannot make a blanket statement, I can update -- I can dynamically update without any problem. That would -- a POSA would say, wow, really?

So, again, like I said, basically, you have to scope the problem and say, by database I mean this, and by scenario, I mean this. I mean, are you using the same data in memory? If that's the case, how do you synchronize the data copy you have in memory versus the data copy you are updating in your storage. That's a super hard problem.

Q Is there a SQL command for inserting data into a table?

A Yes, of course, yes.

Q What is it?

A It's -- it's I think called insert. You can create table and insert or add. I don't remember, yeah.

Q So when you insert the data --

A Yeah.

Q -- is the database online?

A Online means what?

Q It's operating.

A So, again, database, a strict computer science definition of database is organized file system. You will not say the file system itself is the application. The application is the one that uses the data. That's two separate thing. You say, oh, isn't that life? Depends. I mean is file live, yeah, you can access it, but if the file system the data just fly straight in your face automatically, no, you -- you have a software or application, that process data, that's called database management system, okay.

So I can tell you that for inserting a database table -- you can look it up -- two-phase commit or -- or locking. When I update the table, nobody can touch the table, nobody can touch the table. I'm going to -- I'm going to basically lock the table and say nobody have access it. Clear or clear, I insert, then release -- release the lock. That really tells you -- you cannot release the update -- the basic database.

MR. GOLDBERG: That really tells you.

A That really tells you the basic database principle, when you update the data, what you do the two-phase locking, two-phase commit? You could because you don't want another -- you don't want your database application to read the data while you're updating it. It's like I will withdraw 100 bucks. At the same time I want to -- I want to withdraw another 100 bucks, but you only have 100 bucks in your account. You cannot do -- you cannot allow these two -- two transactions to happen at the same time. That's updating database. So you say, okay, say, Nolan, say you go -- so let's say Nolan say I want to update database. So if Nolan says I want to update the database.

Q Noran?

A Nolan. I want to update the database. I want to withdraw hundred bucks, okay. That's updating database. The first thing I want to do is I want to have a lock of the record. Nobody can touch that, okay? Then you -- then Nolan

would withdraw 100 bucks, now the account is zero. Then say, okay, I'm done. I release it. Then if I want to go there and withdraw 100 bucks, they say no, you're out. There is no -- no -- no money is available. So this kind of locking tells you that they want to prevent data being, kind of, so-called race -- race condition. That tells you updating dynamic updating is so hard for you to claim, oh, I can dynamic update database. If you're a bank, you don't want to do that. You want every single update to be based on data that you know is a ground truth, nobody touching it, okay?

You don't want inconsistency, basically. Otherwise, if you operate a bank, the account can be withdrawn and you're negative, whatever. So that's -- like I said, a basic database principle. Any -- any POSA, any computer science student would have learned that to say dynamic operating database, wow, what context?

It's like race condition, let's talk about. It's a perpetually hard problem in

computer science. People try to stay away from it by what doing locking and don't mess with it in a particular database, okay?

Q Do you know what an insert command is in SQL?

A Same thing, I can insert 100 bucks.

Q Okay.

A Okay. Whatever.

Q Do you know what a query command is in SQL?

A Yes, select.

Q Can you run an insert command, then a query command to retrieve that data without turning off the database and turning it back on?

MR. GOLDBERG: Objection to scope.

A No. Any time you update the database, like insert, delete, you want to lock.

Q That wasn't my question, sir. My question was, can you run an insert demand to insert data, then run a query command to retrieve that data without shutting off the data and turning it back on?

MR. GOLDBERG: Objection. Scope. Asked and answered.

A So like I said, depending on what shutting off means. Basically locking it is an equivalent of shutting off that table so nobody can touch it. So when you select, you guarantee that you're selecting based on the what we call ground truth result, meaning that something is inserted into it.

Yeah, you want to basically -- it's called integrity, integrity of database. You want to ensure that database remains, the integrity is always guaranteed while you're allowing the updates, and the only way you do this is you lock up other possible concurrent -- concurrent access to it. So when you lock the database, database table, that's something similar to shutting it -- shutting down that particular table so nobody can touch it except you.

Q Wait, when you -- if you're going to lock a table to do, like, a write for data integrity and then a retrieve, locking a table is not the

same as shutting down a table?

MR. GOLDBERG: Objection to form.

A So --

Q Turning it off, right?

A What I'm trying to say is when you're locking that means no nobody else can. Before you do an insert or delete, you acquire -- acquire the lock of the table.

Q Inquire?

A Acquire, you want a lock -- acquire.

Q Acquire. I'm trying to help the court reporter out.

A Acquire, acquire a lock on the table. That means essentially shutting it off to everybody else except to you. Okay? Then you finish your update, then release a lock. Now that's equivalent of bringing back alive so other people can access it. A POSA would understand that's how a database operates.

Q While you do that lock, you don't need to turn the database off and turn it back on, the database is still operating, right?

MR. GOLDBERG: Objection to form.

A So, again, you're confusing database application with database as data. Like I said, database is essentially a hierarchical file system. Is a file system alive? If someone can access it, that's alive. But what is shutting down a file system mean?

Q All right. How about this, I think I understand what you're saying. When you write to a particular table, you have to lock that table for data integrity or lock the particular field, whatever, before you can pull it out. So if you're writing data to one table, can you read from another table while that data is writing?

MR. GOLDBERG: Objection. Scope.

A Yeah, as long as it doesn't touch that table, yeah, so...

Q And once the data is done writing in that first table, can you retrieve that data without shutting off the database?

MR. GOLDBERG: Objection. Scope.

A Like I said, I never say about -- so

database application and database are two different thing. Database normally would mean the storage of data, and database application means -- the -- the operation that you -- that you -- that you apply on the data, okay?

So my point is that when I say lock those table, nobody can access it. That means other database application essentially being shut off. They can't access this table. So the -- the equivalent -- the equivalence is basically shutting down those applications if they do not want this data -- this particular table. That's the same equivalent, yeah.

Q So let's imagine a simple database that has two tables, okay?

A Yeah.

Q We'll call it a first table and second table, okay?

A Mm-hmm.

Q Then you're going to have a database application that's able to read and write to those tables, okay?

A Mm-hmm.
Q So your database application, you can write to the first table and read from the second table, right?
MR. GOLDBERG: Objection to form.
A Okay.
Q Can you do that?
A Can you repeat the question? I mean, I'm a little bit confused how you describe it.
Q From the database application, you could write to the first table and read from the second table while the first table is locked, right?
MR. GOLDBERG: Objection to form.
A So, again, it depends on the data dependency. So if some -- Table 2 depends on Table 1 data, you have to lock everything, yeah.
Q So let's imagine a scenario in which there is no data dependency between Table 1 and Table 2, okay?
A Mm-hmm.
Q With your database application, can you write to Table 1 and read from Table 2 while

table -- the first table is locked?

MR. GOLDBERG: Objection. Scope. Form.

A So, so, again, -- so like I said, so really all this updating situation really depends on the context of how you define updating. So to me your situation is almost like, yeah, application is reading this data, but doesn't use that data. You can update all day long. This is almost like you're talking about two different system now, meaning when I lock this table, the database application they rely on this table would be essentially being shut down, because it can't access this data even though they want it. That's what I'm talking about the updating is not -- dynamic updating is not always possible. The situation that you try to say is, yeah, if I don't use data -- you can update data, right, because I don't use it. That means I don't know what is analogy here, it's almost like that database table is not something that belongs to an application anyway, so I can happily let do you whatever. That's -- but that's not in general what we

understand dynamic updated database. I mean, dynamic updating database would not be a hard problem if you don't rely on the data. That's not a hard problem. The hard problem is that you rely on a data and then when it's being updated you essentially have to be essentially shut down in order to not create inconsistency.

Q All right. So first of all, like I have a very specific example where I'm talking about a single database with two tables and a database application where you have your database application write to the first table, can you read from the second table while the first table is locked? That's the simple question that I'm asking you. Can that be done?

MR. GOLDBERG: Objection. Form. Argumentative. Asked and answered.

A So, again, in a lot of database, if you read the -- the -- the spec, normally the preferred implementation is that while you're updating -- because you already acquired the lock, you're using a lock, you want to finish that job,

release the lock, before you do anything else. That's not just for efficiency purposes. It's essential fairness thing, meaning that -- fairness, meaning that you don't have the lock and say I'm going to take my time, who cares you're waiting. No, that's normally not a kosher thing to do. So, again, for you to say, while it's -- while it's being updated, while I have the lock, I do something different, I don't know which database management system would want you to do that or would allow you to do that. So I mean your example is just weird.

Q So is it your testimony, as you sit here today, that there are no databases -- database applications that could write to a first table and read from a second table while that first table is locked? Is that your testimony or that doesn't happen?

MR. GOLDBERG: Objection. Form. Mischaracterizes prior testimony.

A So like I said, in general, that would be a very bad practice. That would create a

potential situation of debt lock problem. People -- that people spending their whole career studying it. Yeah, so that's why normally the practice is do it single thing, in particular locking. You want it to basically lock, do your work, release the lock. Basically, you say, hey, I have the lock, I'm going to do something else, then I'm going to create some other situation that requires some additional locking, are you waiting for somebody else to lock, that really becomes, you know, untenable situation. So that's why you can point me to a database system that allows you to do that, but I would say that's bad practice.

MR. GOLDBERG: Jonathan, we've been going almost about an hour, so when you hit a point.

MR. TUMINARO: Now is a good time. Let's take a break.

MR. GOLDBERG: We should have a lunch break, I think. The food's here.

MR. TUMINARO: Okay.

(Luncheon recess)

BY MR. TUMINARO:

Q Welcome back, Dr. Lee.

A Yeah.

Q Before the break we were talking about databases. I just want to follow up on a couple things. One of the features of commercially available databases in the '90s was the ability to connect to multiple clients; is that right?

MR. GOLDBERG: Objection. Form. Scope.

A Again, it depends on the application, right? So let's say the database that a bank uses, yeah, you would consider we have multiple ways to connect the database, right, because even the -- sorry, even transaction that you initiate at a branch -- at a bank branch when you want to update the data in a database, right? So you can imagine multiple branches would be able to send updates to the database. In that sense, yes, you can accept multiple -- you can -- in that case, the database can accept multiple distributed clients.

Q Okay.

A Yeah.

Q So I'm imagining a scenario in which a database accepts multiple distributed clients. The database has, let's just say, two tables for now, just to make it simple. So client A writes to the first table in the database. Are all of the other clients locked out or have -- the databases inaccessible to all the other clients while client A is writing to Table 1 in the database?

MR. GOLDBERG: Objection to form. Hypothetical. Outside the scope.

A So like I said, if database table A is being locked, that means, you know, none of the applications except the one who is updating, who is locking the database table A or having the lock, none of the database can access it. So in the context of Table A, that's equivalent of all these other database applications or modules being shut down or being kind of, you know, stopped from database A until the lock is released. Then it can resume.

Q But I guess what I'm asking about in

particular, like client -- client one is writing -- or client A is writing to Table 1. Are all of the other clients, are they -- is the database inaccessible to all of the other clients while client one is writing to Table A?

MR. GOLDBERG: Objection. Form. Hypothetical. Scope.

A So in your -- in your example, right, if let's say other -- all the other clients are accessing data that is not in Table A and have no relationship with Table A, yeah, I can imagine they can operate, but I would argue that a POSITA would also say in this situation, it's almost like Table A and the rest, they're completely two different database, and that's why all other client can, say, still work while you're updating this database A.

Q Okay.

A So Table A. So what I'm trying to say is that for application database that rely on Table A, then while it's being updated, you're essentially being shut down. That's what the

whole point. That's why I kept saying before the break that when you say database updating, exactly what do you mean referring to -- if you want to scope it, scope it, a proper scope, I really think it's fair to say that your situation is equivalent of all the other clients, and this client, they're essentially operating in two different database, one is Table A and the rest.

So when you say -- you say the dynamic updating doesn't affect me, if you say dynamic updates doesn't affect me, that's because you're, in fact, operating in a different database.

Q Okay. So now what about the scenario where client one or client A is writing to Table 1. Is Table 1 inaccessible to all the other clients where client A is writing to that table?

MR. GOLDBERG: Objection. Hypothetical. Form. Scope.

A So like I said, in general, when you try to update a database, you want to acquire, acquire a lock, hold them to the lock while you're doing the update. And then when you finish, you know,

you basically finish an update, database will let you know, yes, the updated -- the data is updated, then you release the lock. The point is that in this period, when you have the lock, nobody can access that table. No client other than yourself doing update. So like I said, that's equivalent of saying that when a database is being updated, your application that rely on the data is being shut down basically until the update is finished.

Q So is your understanding of what dynamically modifying means that -- what is your understanding of what dynamically modifying means?

MR. GOLDBERG: Objection to form.

A So I really think that for database because, in particular, the -- a lot of database like the example that we are using that -- that accepts multiple distributor clients, then updating becomes super challenging without running into, potentially, problems with consistency. Okay. So that's why when you say database updating, I want to know the exact scope before I can comment whether that's possible or not.

Q So dynamically updating is a super challenging problem?

A As we have gone over. Like I said, your example would be, you don't have to touch database one, yeah, you allow it to be updated because you're working on everything else. That's -- a POSA would agree, that's equivalent to having two separate database. Everything else, working on this database and while this database -- this other database updated, you're not touching it anyway, so you are you're not affected so. So which means that because the equivalents is you're operating -- you're having two different databases -- update this database, of course nothing to do with -- with this other clients, they're actually in fact -- in fact working on different database. That's how I see it.

Q Is it your testimony that a person of ordinary skill in the art would not know how to dynamically update data while something was online because it's a super challenging problem?

MR. GOLDBERG: Objection.

Mischaracterizes prior testimony. Scope.

A Yeah, like I said, it was super challenging problem. I don't remember how many students, you know, friends of mine who are doing database research at the time, writing a thesis about all these kinds of updates, consistency, I mean, I think it's a super, super challenging problem. If you say is this -- something possible, like I said, maybe some specific situation with the proper context, it's possible, but again, like I said, I can only opine if you give me the description of that particular situation.

Q Well, let's look at what the '641 patent says about dynamically updating.

A Okay.

Q If you turn with me to Column 5.

A Okay.

Q Line 32.

A Okay.

Q And with respect to this super challenging problem, the '641 patent says, "The software and

filters of probe/sentry system 2000, in a preferred embodiment, may be adaptive or, alternatively, may be manually updated offline or dynamically. That is, during actual operation."

So is it your testimony that those three words, "during actual operation," is sufficient to teach a POSA how to do this super challenging problem of dynamically updating?

MR. GOLDBERG: Objection to form. Argumentative.

A Let me see.

MR. GOLDBERG: Scope.

A Yeah, so, again, what '641 patent teaches, right, Column 5, starting Line 32, is very different from the example that we talked about having a database having multiple -- having multiple distributed clients who want to access the same data. And the challenge there, like I read, discusses that if you update, one client wants to update, then what about other clients rely on the same data? That creates some problem.

But I think from what I read here in the

'641 patent is different. You just -- basically, you update the sensor, let's say update the rules that are used by this probe. It's not like you have multiple updates coming to the same place. So it's easier to manage the consistency problem.

Q How is the -- the -- when the probe is doing its filtering, it's going to be using some sort of rule, right?

A Yes.

Q How do you solve this consistent -- super-challenging consistency problem of using a rule that might be updated at the probe when all the '641 patent says is you either do it offline or dynamically? It doesn't give any details about how you do that dynamically. How is a POSA supposed to understand that?

MR. GOLDBERG: Objection to form. Argumentative.

A So a POSA would tell you that to implement this kind of a probe, when you -- the software brings up, you read a configure file that has all the rules -- all the filtering rules. And it

needs -- a POSA would read this and say, oh, I see I can basically send a ping or something -- a ping.

Q P-I-N-G.

A Yeah, a ping message to the system, say, hey, the config file has been updated, just read the config file again. So that's relatively straightforward because, again, you're talking about a single update from one place, you know, from one sourced update that probe.

It's very different from what is describe the database when you have multiple, you know, clients and update and all these synchronization problem that you may run into.

Q So in that scenario, the probe would have to be able to -- or you'd have to be able to write a new rule to the probe while the probe is still collecting data, right?

MR. GOLDBERG: Objection. Form.

A Yeah, so it's like this. So you basically --

Q Can you answer my question first?

A Well, I mean, I'm trying to explain how this thing works.

MR. GOLDBERG: Are you withdrawing your prior question? Because he was answering.

MR. TUMINARO: I don't think he was.

A Can you repeat the question?

Q Yeah. The probe would have to be while -- you're writing a new rule to the probe, the probe would still be collecting data, right?

MR. GOLDBERG: Objection. Form.

A So the probe works as a collect data in their prior rules, okay? So I mean, a POSA -- the way I would -- I would implement this is, yes, collecting the data while I am loading the updated config file. It doesn't mean that whenever -- whatever you just collecting would not be -- would not be -- would not be -- would not be using the updating rules.

In computer science there is a concept called buffering. Whatever you collected, you can put a buffer while you're updating, you know, reading the config file updating memory, and then

you just apply your rules in the data that you collected. I mean, in fact without updating the data that you collect, you normally put in a buffer while you are applying the filtering rules. So it's nothing -- yeah, nothing difficult here in terms of if you want to do this. A mean, POSA would figure out a way to do it.

Q So the way the POSA is figuring out how to do this dynamically updating, is -- the way I understand it is that the rule is being written not while at the same time that it's being applied, right?

A So think about this, there is a single CPU. CPU can only do one thing at a time. You either collect data or you apply rule. You cannot do both at the same single instant of time. There is only one CPU, yes, so that's what I'm trying to say. You can collect data, put the buffer, and then you also next whatever -- next epoch, epoch of time, you update the rule and you go back and apply the rules to the -- to the data. That's a well-known thing in computer science is that the

CPU may give the impression that doing same things at the time, but every single moment does only one thing.

So, basically, it's just okay doing step, doing one, and then doing two, doing three, and then the aggregate of time you feel like it in parallel, but they're not. In the sort of long enough time, even though you feel like everything is doing in parallel. But actually it's not, every single moment is one thing. That's why I'm trying to say you cannot say you collect data while you're applying the rules at the same moment. You cannot. You either collect or you apply the rules. Two things.

Q How is that any different than the concept of dynamically modifying a database where at the time where you're writing to a table, you lock it, then during the next epoch of time, you can access the data and that would still be dynamically modifying the database. How is that any different than the scenario that you just talked about of being dynamically modifying?

MR. GOLDBERG: Objection. Scope epoch.

A So like I said, in a database situation, you lock it, and that normally lasts more than, you know, a couple epochs. The point is when you lock it, you completely cannot access the data.

Q What's the duration of an epoch?

A Depending on the updates.

Q So how is that -- like, the epoch of a config file any different than the epoch of a database?

MR. GOLDBERG: Objection to scope. Form.

A So like I said, I think I only said this, right, in the four -- '641 patent, I do not see a need to lock it because you don't have any concurrency I worry about. It's different from database situation. So in database situation, you lock it because there is a consistency situation that you have to worry about. And like I said, when you lock the table, you cannot even access it and you know the data that you are using is completely not reliable. So you basically -- you basically -- essentially, you're being shut down

and then starting after the lock is released.

Q How many epochs does it take to read and parse a config file in the dynamic modifying that you're talking about for the analysis capability of the probe?

MR. GOLDBERG: Objection to form. Hypothetical. Scope.

A So, again, depends on how big the update is and how fast you can read the config file, right? Yeah, but like I said, in general, you know, you cannot do multiple things at a single time anyway, so you, basically, this epoch you read data, this epoch you apply the rules, this epoch maybe you see what it's updating. Anyway, then the CPU says, okay, these three tasks in aggregate of time, you think they're in parallel, but, you know, so to me a POSA will understand that's how it works.

Q So would the epoch for reading and parsing a config file be more than one -- more than one epoch?

MR. GOLDBERG: Objection. Form.

Hypothetical. Scope.

A So, again, it really depends on how much -- how big that data is.

Q And how many epochs would it take to write to a database table?

MR. GOLDBERG: Objection. Form. Hypothetical. Scope.

A So, again, it really depends on the -- on, you know, how big the update is. Yeah. So.

Q What you just described with respect to the dynamically updating a probe, you said during one epoch you read, one epoch you then apply the rules, and over a longer period of time, it seems like it's all in parallel.

The same thing for a database, couldn't you have in one epoch you're writing the data and then in a later epoch you're reading the data and then over a period of time, it seems like it's happening in parallel?

A Yes, I mean, sure, if the window is long enough, you feel everything is in parallel, but in reality, my point is that locking things out is

fundamentally a much bigger operation, much bigger impact of the operation than what we described here, right? So meaning that when you lock the table, you -- basically, nothing of the table you can access. So if your application, if your database application relies on data from that -- that table for -- then for what understand of database application essentially you're being just -- basically, you're being stopped until the lock is released. Then you -- then you can resume. So it's much bigger operation, bigger impact than what we talked about here.

Q While you're updating a config file for a probe, you can't apply that config file while it's being updated, right?

MR. GOLDBERG: Objection. Hypothetical. Form. Scope.

A So, again, these are implementation details which, again, as -- you can ask a POSA there are multiple ways to optimize it.

Q My question is simple. Can you read the -- or access the config file while it's being

updated. It's locked essentially, right?

A No.

MR. GOLDBERG: Same objections.

A You don't have to lock in UNIX is whatever reads or writes last is the last laugh. Anyway, that's details here. For example, the update message can say, hey, ping you, update, rule number hundred. Maybe -- maybe the POSA, okay, fine, I don't need to use it right now, I don't have to spend all my cycles doing whatever. So the whole situation like that, it's not like database when you lock, the whole database is locked. It's the way the database is organized. It's basically a hierarchical file system. It's -- it's very hard to say, oh, I only want to lock only data record, everything else you can access. That's not how you work in database. It's not so simple.

So that's why database locking is very different from what we talk about here. Like I said, you know, it's multiple ways to optimize so that you don't have to sit there and wait forever

for the config file to be updated. You probably don't. It depend on, like I said, how big the update is and what kind of information that you can utilize to minimize the wait.

Q So in your opinion, the fact that the probe may be not be applying the rule for some period of time while it's updating doesn't mean that the probe is -- isn't dynamically updating?

MR. GOLDBERG: Objection. Form.

A So like I said, imagine the probe will say I spend, you know, let's say one -- one out of every third epoch to read the updates. Then if you say, okay, then when the next epoch comes, then it's the probe's turn to apply the rules, can they do it, yes. If the update is Rule No. 100, I'm using Rule No. 10, of course I can go ahead and do it.

So, again, like I said, there are multiple ways to organize information and tell the probe whether it needs to wait or whether it can go ahead and apply the rules, meaning there are ways to tell the probe that the rules it already has is

not updated, go ahead use it.

Q Just to be clear, when you're saying dynamically updating the probe you're not saying the update is occurring at exactly the same time that the data is being collected, right?

A But what answer that question. This cannot be true in a modern day computer, right, only one CPU, one epoch only belongs to one thing. So we can't have the exact same epoch doing multiple things.

So we -- you cannot do more than one thing per epoch. You can do only one thing.

Q If you don't have a parallel processor or something.

But just to be clear, I understand your testimony. What you're saying for dynamically modifying it requires then in a first epoch you're updating, and then in some later epoch you're applying that update, but it's occurring on such a time scale that it appears to be dynamically or it appears to be in parallel.

Is that what you're saying?

MR. GOLDBERG: Objection. Misstates prior testimony. Scope.

A So what I'm trying to say is that a POSA would know how to implement this so that the config file can be updated and the necessary changes can be reflected in the probes in memory while it is still running and applying the rules to the data. I mean that's all I can say, yeah.

Q And the '641 patent doesn't provide any implementation details for how to dynamically update the probe's capability?

A Let me see. I mean, let me see an example or not. Let me see if my report has this.

Yeah, I mean, I can't find a specific examples in the -- in the patent or in my report, but like I -- like I already said, a POSA reading this would -- would, you know, understand how it works and implement it.

Q So the rules for updating the config file are stored in memory; is that right?

A Can you repeat the question?

Q The rules -- sorry, the rules for the

config files or the rules that are applied by the probe, those are stored in memory, right?

MR. GOLDBERG: Objection. Form.

A So a POSA would agree that when a probe applies filters, yeah, the filters have been read from a file and then it's in memory, yes.

Q Okay. And while the rule is being changed or updated in memory, it can't be applied, right?

A So, again, depends on which rule I'm meaning, that, again, if you say, hey, I'm updating Rule No. 100, then the probe say, at this point I'm only -- I'm applying Rule No. 10, yeah, I can go ahead and apply whatever copy I have.

Q That wasn't my question. Let's say a specific rule is being updated. During the epoch where that rule is being updated, during that epoch, it cannot be applied, right?

A So like I said, the CPU can do one thing at a time. If that epoch is reserved for being tasked to update a rule, of course you can only do one thing, updating the rule. You're not applying. You cannot do both updating and

applying at the same time, so.

Q So during that epoch where the rule is being updated it's essentially locked, right?

A I wouldn't say -- I wouldn't say -- I wouldn't equate the concept or notion to locking database sense. Then it doesn't mean that CPU every single epoch is locked. No, we don't talk about that term. We don't use that term.

Q You don't use that term. During the epoch where the rule is being updated, that rule cannot be applied, right?

A Like I said, you only do one thing at a time. If that epoch is doing updating, then you're just doing updating. You don't do -- you do not -- it cannot do anything else in the epoch.

Q Just to be clear, when you say "epoch," you're talking about, like, a single operation happens during a single epoch; is that right?

MR. GOLDBERG: Objection. Form.

A So what epoch means that any instant of time, how many infinitessimal you want to define, meaning that a CPU only operates one instruction

at a time.

Q So --

A So if that instruction is updating, you cannot do, oh, that -- this instruction does both updating and applying. No. It doesn't work that way. It's really in a single instruction level I'm talking about.

Q That's what I'm trying to understand.

A Yeah.

Q When you're saying epoch, what you mean is during a single epoch a single operation occurs?

A Well, so there is more nuance to that. Like I said, there's a lot of these application -- details. In fact, you can say, hey, does this -- it really depends on how CPU and operating system are implemented to say do I give, you know, this particular task multiple time for doing multiple instructions with a single instruction. Those are just information details. But a concept is that you only do one thing at a time.

Q Okay. Can we go to Page 12 of your declaration.

A Okay.

Q In the middle of Page 12, you have the heading that says, "Petitioner's experts assumption that Duvall would be used for security is not an assumption a POSITA would make."

Do you see that?

A Yes, I see that.

Q Do you stand by that statement?

A Yes.

Q The claims of the '641 patent don't require use for security, right?

A Can you repeat that question again?

Q The claims for the '641 patent don't require use for security; is that right?

MR. GOLDBERG: Objection. Form.

A I don't quite catch the last few words. What do you mean by "use for security"? What do you mean?

Q Well, you used the words that -- that Duvall -- that a person of ordinary skill in the art wouldn't assume that Duvall would be used for security, would be used in a security context, is

what I understand, but the claims don't require use in security, right?

MR. GOLDBERG: Objection to form.

A Well, I mean, Claim 1 talks about -- I mean Claim 1, right, look at it and say, a system for operating a probe as part of a security monitoring system for computer network. So, obviously, this patent is about -- is basically for -- whatever the patent is teaching is for use for security purposes.

Q Well, looking at Figure 1 -- I mean Element 1B, what the filtering subsystem does is it analyzes status data to identify potentially security-related events, right?

A Yes.

Q It doesn't require the identification of security events, right?

A Well, I would say that potential -- potentially security-related events include security events.

Q Well, it's not even security events, it's security-related events, right?

A I would say security-related events a superset of security events. It would include security events. It's self-related, meaning that security-related events should include security events. That's how a POSA would understand.

Q It's not even limited to, like, actual security events. It's potentially security-related events, right?

A That's what it said, yeah, potentially security-related events, yeah, okay. And then that's why you want to do post-filtering analysis, so on and forth, so yeah, and then identify, send information about the identified events to another system. That's 1C, yeah. So, basically, the point is everything that he teaches, 1B, 1C, is all about security.

Q And you would agree with me that downloading a porn site, information from a porn site is a potentially security-related event, right?

MR. GOLDBERG: Objection to form.

A I would think everything is potentially

related to security, including your email, including PDF documents. If you go that route, anything you touch, open up your computer, connect to Internet, potentially you be infected. You want to go that route, yeah, everything is potentially.

Q So filtering obscene material is like a sort of narrower set of something that can be potentially security-related event, right?

MR. GOLDBERG: Objection. Form.

A Can you repeat the question again?

Q You said that, "anything you touch, email, could be a potentially security-related event."

So what my question is, if all of this could be a potentially security-related event, the specific task of filtering obscene material, like a porn site is a potentially security-related event, right?

MR. GOLDBERG: Objection. Misstates prior testimony.

A Yeah, again, so I mean, I think I said this in -- in the -- in my declaration, but again,

let me see. There is a lot of context. So let me just see here. (Document review.)

So, I mean, I think I already opined this in my report, I think starting paragraph 31 all way through paragraph 41. So -- so really at a high level, the point is that, like I say, anything potentially can have security implications. That's exactly why I talk about, you know, in Figure 1 and Figure 2 of this '641 patent that you have all kinds of negative filtering, positive filtering, and post -- analysis of post-filtering residues. So essentially you're looking at the contextual information. You don't say, wow, this is porn. You look at other contextual information to say is this reasonable thing to do? Yeah, I mean, so as I said in my report here, that -- let me point to some specific language I use.

So I would say that -- I mean, I would -- basically in paragraph 36, I said, look, I mean the -- I said that, you know, sometimes objectionable content may pose a risk, but it's

like everything else, even the nonobjectionable materials such as email may sometimes actually pose a risk. And -- and the point is that, as I said in the next sentence, right, the petitioner's expert has not provided any evidence of any actual correlation between objectionable materials and security risk.

And the next sentence say, you know, for example, right, you say what objectionable, well, you know, the example would be just because a website has a curse word, it means it has a virus. That's -- that's a leap that a POSA would not make, and a POSA would say, okay, curse word, so what? If you have some other circumstantial evidence that tells me, normally I can tell -- can tell you security guy would say, this website objectionable content or not, this website is known for hosting malware. Don't go there. That's normally what security POSA would tell you.

A POSA normally would not say don't go there because it's porn. No. We look at information, evidence that that's

security-related, not just because there is curse word. Okay? So that's really -- so my point really is that a POSA in security would find it odd to look at Duvall's and incorporate Duvall's teaching. A POSA would not just look at Duvall's patents and say, oh, I'm going to incorporate this into security monitoring, because it's talking about very different things.

Q So I lived through the '90s. You lived through the '90s. You know that, like, at that time, it was well-known that pornographic sites were very susceptible to having malware and spyware and viruses, right?

MR. GOLDBERG: Objection. Form.

A That's not what I remember, no. That's -- that's not how I remember it.

Q It's your testimony, as you sit here right now, that porn sites were not -- visiting porn sites, downloading materials from porn sites, was not a security risk?

A That's not what I said. I said that, first of all, I don't remember specific things

calling up porn sites as a place where you get infected. In fact, I clearly remember porn sites among the first sites that implement secure SOC layer because they want to charge you. They want you to pay to get some contents.

In fact, I would say that a driver for a lot of web security technology that we know of today. Just like VCR. That's a complete side note. Not just saying because you want VCR, you want to watch porno that you get yourself. In fact, it's completely -- to me, it's crazy notion that I do not know, okay? Like I said, the way I remember the '90s when the -- porn sites in the '90s, they were the first one to say I want to -- I want you to pay. In fact, it was underground discussion, say, oh, how do I steal my dad's credit card number and enter without him knowing, crazy things like that.

So like I said, to say going to porn site you get infected is completely opposite to what I know. Okay. So like I said, nobody in POSA know of to say, oh, porn site you should avoid because

it's a security risk. That's very foreign to me.

Q Are you saying that it wouldn't be relevant to network security to block certain websites?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony.

A So it doesn't work in this space. I can tell you that most of the time when we block a website is because we know this website. Normally two things, it's used to do command and control, meaning that command and control, you actually visit website where your infected machine would talk to and say, hey, what do I do today, what kind of spam do you want me to send? So you want to block traffic to those so-called command control sites.

Another kind of site that you know you should block is this site is known for hosting malware. You don't want your machine to go there and download malware.

Maybe the third kind meaning this website is known to be compromised. So when you visit,

loading a page from that website, your browser can be compromised. Again, the gist is that you want to block a site if this site is known for doing bad things. Porno by itself is not known to doing bad things to security, at least that's not I know. You can point me to article that specifically talks about, oh, don't go to porno site because security. That would be awesome teaching tool to go to school.

Q But you would agree with me that blocking websites is a relevant concern in network security, right?

MR. GOLDBERG: Objection. Form.

A I think I only answer the question, blocking sites normally they are known to be involved in malicious activities or have a bad reputation -- we actually did at least one or two piece students doing their thesis on the topic to say why should you not go to website? Normally like I said, based on evidence of bad things or guilty by association, meaning that, yeah, it's in this neighborhood, this machine that's known for

bad things. So if this website is hosted on the same machine, don't go there.

So, again, we look for evidence data security-related evidence or information, not just say, oh, porno, whatever. Again, it's very, I wouldn't even say interesting concept. So foreign to me. A POSA would have a hard time understanding why they would apply Duvall for security for that same reason.

Q So it's your testimony that porn sites do not have potentially -- downloading material from porn sites does not have a potentially security-related threat?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony.

BY MR. TUMINARO:

Q Let me --

A That's not what I said.

Q Let me rephrase because my question was bad.

A Okay. Go ahead. Rephrase it.

Q Is it -- so is it your testimony that

downloading material from a porn site does not pose a potentially security-related threat?

MR. GOLDBERG: Same objection.

A First of all, that's not what I said. Second of all, I'm not a big fan of porn site. Third thing is you never download material from porn site. You get into some other kind of trouble. Let's leave it at that.

My point is for security concern, yeah, downloading anything from anywhere is a potential non-zero probability that something is bad, but on the other hand as a security person you cannot say, well, how do I secure my machine? Don't connect to the Internet. Duh. No USBs, duh. What do you do? Do nothing. Then the machine will be secure. Come on.

So my point is secure people will know -- a POSA will tell you I want to monitor everything, but I'm using evidence, information, knowledge, and experience, other sources of information, even your insights or connection to underground world, whatever, to basically collect enough

security-related intelligence so you can decide what to block, what to allow. I mean, that's exactly -- and then if you're not sure, that's when you do the post filtering, you analyze the post-filtering residue and sometimes even ask the SOC to help. That's exactly what people are doing, a POSA would understand.

So my point is you don't necessarily say, well, I want you block porn sites. I have no problem with that from an educational point of view, but security point of view, I wouldn't -- I don't know what POSA -- which POSA would say it that way, because like I said, it's an unrelated kind of concept.

Q Do you remember what my question was?

A Whatever your question is, you are saying that -- you're asking whether downloading porn site would or would or would not introduce security risk. I'm saying that anything introduces -- you download has a non-zero probability that something could be bad. But you cannot say, hey, because of that I'm going to

block everything. That's non-zero probability, then block everything. And no security practice would actually be realistic that way. So that's what I'm trying to say is that your question is kind of very ill formed in the sense that a POSA would completely object to your question and say, hey, look, we know what we're doing. We use a lot of intelligence we gather to do the proper filtering and post filtering analysis of -- analysis of post-filtering residue. I use contextual information, knowledge information to decide what to block, what not to block. You can never say just because porno sites are blocked. That's completely irrelevant to the security operation that a POSA would understand.

Q '641 patent doesn't say how to identify potentially interesting events or how to discard uninteresting events, right?

MR. GOLDBERG: Objection. Form.

A So I think we went through this when we went to Column A, right, starting, you know, Line 51, we talk about what it means by -- what it

means by negative filtering, which means discarding uninteresting information, right, and positive filtering means select possibly interesting information. So like I said, a POSA would say, yeah, that's exactly what we're doing in secure monitoring.

Q But my question is the '641 patent doesn't identify what are the necessarily interesting things and what are the necessarily uninteresting things, right?

MR. GOLDBERG: Objection to form.

BY MR. TUMINARO:

Q It doesn't specify what those are?

A So a POSA would tell you the following -- really a POSA, first of all, knows how to implement all these filtering negative or positive.

Second thing is that exactly what filter you put in -- that's called mechanism -- the mechanism normally depends on policy, meaning you as an organization tell me what do you want to allow, what you don't want to allow. I'm going to

implement those. I'm going to implement specific filtering rules according to a policy. That's security 101. You start with a threat analysis, meaning one of the threats to the organization. Then you find policy to say what's allowed, what's not allowed. Then you implement the mechanism to enforce that policy. That's a security 101. You say, tell me exactly what filter is, what filtering rules. Tell me exactly your threats to your organization. Tell me exactly the policy you have, then you'll know how to implement. That's the security 101 they would teach, and I believe that's how people practice it.

Q And there would be no technical restriction that would stop a user from implementing a security policy in Duvall that would block certain websites that the security person wanted to block, right?

MR. GOLDBERG: Objection. Form.

A So, again, if the policy say such site you should block, here is why, then yeah, sure, security person can implement those filtering

rules. I mean, some firewalls policy, I know some example to say, you shall not visit Facebook if you're not in marketing department during work hours. Okay, that's a policy. You can implement that. Is it a security policy? I wouldn't say so. Just because a policy to -- to -- it's a policy to block access to a site doesn't mean that it has something to do with security. Just a policy.

Q In Duvall, you can block a website that had a known security problem, right?

A I do not believe Duvall talks about that either. No.

Q That wasn't my question. My question is: In Duvall, you can use Duvall's system to block a website that had a known security problem, right?

MR. GOLDBERG: Objection. Asked and answered.

A So first of all, like I said, Duvall does not talk about security monitoring. Doesn't talk about blocking sites, objectionable contents. It doesn't talk about a site that has security

problems at all. So like I said, can you say, hey, here is specific website, here is specific IP address I want you to block? I suppose you can. But, again, Duvall is talk about objectionable contents. It doesn't talk about blocking access to a site for security.

So, you know, I mean, like I said, a POSA would not say, oh, because of Duvall's teaching now let me modify for security. It's just, like I said, two different things.

Q So Duvall is capable of blocking websites with security-related problems?

MR. GOLDBERG: Objection. Mischaracterizes prior testimony.

A So, again, that's a very broad statement. Like I said, from all I know Duvall talks about allowing access or blocking access, for example, give example about -- about IP address. So if an IP address, particular IP address well-known to be, you know, let's say malware download, sure you can do that, you can block that, but the thing is, Duvall does not talk about the kind of thing that

a POSA would understand for security purposes, the kind of analysis that would enable it to -- to block access to a site based on security-related information. Because all it does is objectionable contents. Like I said, objectionable content is different than security-related information.

Q Can we turn to Page 23 of your report -- of your declaration. I'm sorry.

A Okay.

Q There is a heading in the middle of the page, heading D.

A Okay.

Q I'll read it. It says, "Claims 1 to 25 are valid because Duvall's direct and deferred actions are never applied to the same transmissions."

Do you see that?

A Yes.

Q Do you stand by that testimony?

A Absolutely, yes.

Q What claim limitation does this apply to?

A Yeah, so let's start with Claim 1, right?

So talks about, you know, Claim 1B, right, "a filtering subsystem coupled to analyze status data to identify potentially security-related events that presented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein in the post-filtering residue is the data neither discarded nor selected by filtering."

Okay. So that's 1B.

And I would say clearly, 1B is the same transmission and I would refer you to Figure 2 of six -- of '641, okay? Figure 2 in '641, you talk about sensor data collector, 2010, right, collects status data. Then negative filtering, 2020, throw away things not interesting. Then what remains is being filtered by positive filtering, meaning that things are likely to be interesting for security.

And then residue is being sent to anomaly event detection system. That's the analysis of post-filtering residue. The reason I'm pointing to those figures is that if you look at this flow of data, data from the sensor to negative

filtering, from negative filtering to positive filtering, to anomaly detection, which is post-filtering analysis, the thing to note is that the anomaly detection system here does not take additional data from sensor.

So that's exactly what we meant by post-filtering residue. You're looking at data that has been essentially passed through these filters. It's not looking at additional data. So which really tells you that this really talks about the same -- same transmission. Okay. That's '641.

Whereas Duvall, if you look at -- let me see, I have figure there -- let me see which page. So on Page 9 of my report, okay, that's Figure 3 of Duvall patent. So this talks about essentially the work flow of data filtering start and then first we call it the decision box say data stream opened. If yes, it doesn't do anything, it goes back. It only handles when a data stream is about to open. Then it decides whether the action was deferred action. This is important.

Then if you flip to the next page, Page 10 talks about the deferred action now. Okay. It basically say -- essentially there's a look there. You first compare the direction of transmission, compare the keywords to the beginning of transmission. If matched, go forward? No. Go back. What does go back mean? Continue to compare, continue to get more data. So that's where it tells you, first of all, it's looking at the open connection. Now the connection is open and you keep looking for more data. So that's really not a -- first of all, it's not the same transmission as what -- what '641 patent talks about. And second of all, they fully support that argument, like I said, Figure 3 is about.

Q Are you answering my question or are you just talking?

A I'm answering the question. Is that the reason Duvall is doing -- the Duvall Figure 3 and 4 are not -- are not handling the same transmission? I first gave you the context of '641 that one -- 1B talks about one connection,

one transmission. Duvall is not. I'm giving the evidence.

Q Okay. Do you understand that you're here to answer my questions?

A Yes.

MR. GOLDBERG: Objection. Argumentative.

BY MR. TUMINARO:

Q And do you understand that your counsel can ask you questions when I'm done asking questions? Do you understand that?

MR. GOLDBERG: Objection. Argumentative. And please don't raise your voice to the witness. It's uncalled for.

MR. TUMINARO: I didn't raise my voice. I'm asking him questions.

A First of all, I answered all your questions.

Q Do you remember what my question was?

A You -- you look at -- you asked me to say I do stand by whatever, B, and I said yes. You asked me tell me why, then I explained to you why.

Q That wasn't even my question. My question

was: What claim limitation does this apply to?

A So I start with claim 1B.

Q And then you started talking about Duvall, which is not something I asked you about. So I'd ask that you please answer my questions and then after I'm done, if your counsel wants to ask you questions, he can, but I'm on a time limit and I need you to answer my questions, please.

MR. GOLDBERG: Counsel, you're being argumentative. Wenke, you can answer the questions any which way you want.

MR. TUMINARO: That's not true. He needs to answer my questions.

A First of all --

MR. GOLDBERG: He is absolutely answering your question.

A First of all, you say, which claim. I tell you 1B. Then you basically then say -- essentially.

MR. GOLDBERG: You don't have to engage with him in this argument.

THE WITNESS: Then you say --

MR. GOLDBERG: There is no question.

THE WITNESS: Yeah.

BY MR. TUMINARO:

Q So do you understand that the -- the invention is defined by the claims and not the figures?

A Okay. Yes.

Q Okay. So what language in Element 1B are you pointing to that requires that the same data be positively and negatively filtered?

MR. GOLDBERG: Objection. Asked and answered.

A So 1B talks about "a filtering subsystem to -- to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by analysis of post-filtering residue," okay? "Wherein the post-filtering residue is neither discarded nor selected by filtering." So that's as clear as it states. The analysis post filtering, it's a residue. The residue is from the -- essentially data neither selected not discarded -- neither

discarded nor selected. And discarded means negative filtering. Selected meanings positive filtering. So the point is you're analyzing residue, residue. You're not analyzing new data. You're not analyzing new data from another transmission.

What's residue? Residue, I think we went through this multiple times. So you start with, let's say, data of a transmission. You go through a negative filtering, go through positive filtering. Then you have an analysis of the post-filtering residue. Residue, not new transmission. Okay. So the reason that -- that's why I point you to Figure 2. If you -- my point is that you're still not clear about Claim 1B, Figure 2 says -- you know, clarified that.

Q You'd agree that the filtering subsystem in Element 1B analyzes status data? Do you agree with that?

A So 1B talks about filtering subsystem coupled analyze status data. Yeah.

Q And you agree that the analysis that that

filtering subsystem performs includes two things. It includes filtering and an analysis of a post-filtering residue.

Do you agree with that?

A Well, yeah, so basically analyze status data to identify potential -- potentially security-related events represented in the status data. And then it says, "Analysis includes filtering followed by analysis of post-filtering residue."

Q And the post-filtering residue is not not limited to --

I'll say it again.

The post-filtering residue is not limited to status data, correct?

MR. GOLDBERG: Objection to form.

A That's not what this 1B says.

Q Well, 1B says the, "subsystem is coupled to analyze status data," right?

A Yes.

Q And then later it says the post-filtering residue is data. It doesn't say status data, does

it?

A Well, it says data neither discarded nor selected by filtering.

Q So that data is not limited to status data, right?

MR. GOLDBERG: Objection. Mischaracterizes testimony.

A So, again, it says, "analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering."

Then it says what's filtering? "Filtering is analyzing status data."

Q Maybe -- I --

A Yeah.

MR. GOLDBERG: It's --

MR. TUMINARO: I thought he was done.

MR. GOLDBERG: That's fine.

MR. TUMINARO: Sorry.

A That's the answer.

MR. GOLDBERG: Jonathan, we've been going about an hour again, so when you hit a convenient

point.
BY MR. TUMINARO:
Q So would you agree with me that what the filtering subsystem does is it looks at the status data to positively filter out what's bad in the traffic, negatively filter out what is good, and retain the residue? Do you agree with that?
MR. GOLDBERG: Objection to form.
A I disagree, because filtering, again, filtering, as 1B says is analyzing the status data. So when it does negative filtering, that means throw away uninteresting status data. Positive filtering means identify potentially useful security information from status data. And the residue, again, is what remains. Again, that's status data. I don't know how else we can interpret the claim language and also the teaching of the patent.
Q So I just want to make sure I understand your testimony. You're saying that the filtering subsystem does not look at the status data to filter out what is bad in the traffic, to

negatively filter out what is good, and to retain a residue? You're saying that's not what the filtering subsystem does.

Is that your testimony?

MR. GOLDBERG: Objection. Form, mischaracterizes the testimony.

A What I'm saying that Claim 1B talks about status data.

Q And --

A And data here means status data.

Q And what is filtered by the subsystem, the subsystem looks at the status data to filter out traffic, right?

MR. GOLDBERG: Objection. Mischaracterizes testimony.

A That's not what the patent specifically talks about.

Q So you submitted a declaration in the IPR proceeding that is IPR-2019-01324, right?

A Yes.

Q And in that declaration, I assume that everything -- you try to make it complete, right?

A What do you mean try?

Q You try to make your opinions accurate, truthful, correct?

MR. GOLDBERG: Objection to form.

A Yes, for every declaration, yes.

Q Can you turn with me to Paragraph 17 of your declaration on Page 9.

A Okay.

Q That was in the IPR-2019-01324.

A Okay, yeah.

Q The first sentence of Paragraph 17, you wrote, "One particularly novel feature of the inventions claimed in the '641 patent is the use of a filtering subsystem which looks at status data to positively filter out what is bad in the traffic, negatively filter out what is good, and retain the residue."

Did I read that correctly?

MR. GOLDBERG: Objection. Scope.

A So first of all, retaining the residue is still the status data, and you say, hey, here says look at status data to positively filter out what

is bad in traffic and negatively filter what is good. Yeah, what's wrong with that? So my point is when you talk about filtering, it's a probe. There are multiple kinds of filters. You can say, hey, look's look at status data.

Q Sir, that was not my question.

(Multiple speakers.)

MR. TUMINARO: No, I need to cut him off because -- listen, I asked him did you see that? Now he's talking.

MR. GOLDBERG: Are you withdrawing the question?

(Multiple speakers.)

THE WITNESS: Are you --

MR. TUMINARO: I --

MR. GOLDBERG: He's answering the question.

MR. TUMINARO: He's simply talking.

MR. GOLDBERG: A, you're raising your voice.

MR. TUMINARO: I am.

MR. GOLDBERG: Okay, you are.

THE WITNESS: How I answer without talking? Do you want me to answer the question or not? Allow me to talk.

Q My question was: Did I read that correctly?

A You read the sentence -- you read it correctly --

Q Okay.

A -- as a text. But I tell you what I meant. Do you want me to explain what I meant or not?

Q Your counsel can ask you that question later.

A Okay. You read English. You can put it in the record.

MR. GOLDBERG: You're free to answer any way you want.

Q My question now is, I think you were disputing with me earlier that your -- the filtering subsystem looks at the status data.

Does it filter out status data or does it filter out traffic? Which is it?

MR. GOLDBERG: Objection. Form.

A As I said, okay, 1B, in particular 1B in this context, the filtering subsystem, you're talking about status data. You say, what about bad traffic, like a POSA would tell you, once you tell me this IP is good, the rest of the probe will let the traffic go, go through. If -- if the -- if the filtering subsystem in 1B tells this IP is bad, the rest -- if the filtering subsystem in 1B tells me this IP is bad, then there is other probe. There are other probe. A POSA will tell you -- this is so obvious to any POSA.

Q I guess what I'm -- what I'm really confused about is, I know that the filtering subsystem looks at status data.

We agree on that, right?

A In 1B, in context 1B.

Q Yes, but what I'm confused about, I don't understand what your testimony is. After it looks at the status data, does it filter traffic or does it filter status data? That's my question.

A So what is it? What do you mean by it?

Q The filtering subsystem.
A The filtering subsystem 1B looks at status data.
Q Yes.
A It doesn't mean that no other parts of the probe would take the information and decide and then say, okay, let the traffic go or block. There is a common sense probe -- a common sense POSA would agree, a probe is not a single function, single mode. There is multiple function doing different things.
Q But I'm still confused. Is this filtering subsystem filtering status data or is the filtering subsystem filtering traffic?
MR. GOLDBERG: Objection. Asked and answered.
A I already said, the filtering subsystem.
Q I really don't know what the answer is.
A No, I told you, okay. 1B, according to 1B, works on status data, okay?
What about traffic? Like I said, there are other modules in the probe that would

basically take the -- take the output of filtering system 1B or position from 1B and act on it on traffic, and that's like so obvious any POSA would know that.

Q But so, previously, you said that in Paragraph 17 of your previous declaration that "the filtering subsystem looks at status data to positively filter out what's bad in the traffic." So I'm really confused. I really don't understand your testimony.

Is the filtering subsystem filtering traffic or is it filtering status data?

MR. GOLDBERG: Objection. Scope. Asked and answered.

A So in Paragraph 17 I talk about -- looks at the status data, okay? And then to pause the filter out what's bad in traffic or negative filter, what's good and retain the residue. I mean, like I said, a POSA reading that would say, hey, doesn't have to be the same filtering subsystem as described in 1B that does all of that. 1B -- sorry.

The filtering subsystem in 1B talks about looking at status data, including the post-filtering residue. Then say what about the actual traffic? That's applying what's the -- that's basically applying the decision of the filtering subsystem in the context of 1B on the traffic.

So -- so like any firewall would say here is a rule, say this IP is bad. Then you cause a module in your network to basically cause the operating system to block some traffic. That's a, I would say, implementation of system details that POSA would say, yeah, okay.

MR. GOLDBERG: Let's break.

MR. TUMINARO: Okay.

THE WITNESS: That's another -- see what I'm saying?

MR. TUMINARO: No, I don't. I'm really utterly confused.

MR. GOLDBERG: We're on break.

THE WITNESS: Okay.

(Recess.)

BY MR. TUMINARO:

Q Welcome back, Dr. Lee.

A Yeah.

Q Dr. Lee, before the break, we were talking about the filtering subsystem. I guess it still wasn't clear to me, what is filtered from -- by the filtering subsystem? Is it status data or is it traffic?

MR. GOLDBERG: I'll object as asked and answered.

A Yeah, so as I answered before the break, right, if you look at 1B, it talks about status data.

Q And if status data is what was looked at, is an example of status data, like, an IP address?

A IP address is one example.

Q Okay. So would it be possible that the filtering subsystem and, sort of, an example, you can look at an IP address and, say, oh, that IP address I know is a security threat, so I'm going to filter the data coming from that IP address; is that fair?

A So I think as I tried to explain before the break, so imagine -- I think this same thing -- whatever describing in 1B except the post-filtering residue is actually very common, let's say, for example, a firewall that's both negative and positive filtering. And you say, does the firewall rules that should say this IP is bad versus good. Are they working with status data? Yes, they're working with the status data.

Then they say, what about the traffic that associated with this IP that you should block? Well, the firewall filtering monitor would call this corresponding system function to block the traffic. That's -- that's what I was trying to say, is that the filtering subsystem here is really operating on status data. The effect on traffic can be implemented by calling the specific network module of the operating system say, block that traffic. So that's really an implementation detail depending on what operating system you're using.

Q So then what is the thing -- the thing,

the feature, the name of the thing that's doing the blocking?

A Can you repeat the question again?

Q You said something like it's an implementation detail for how to block the traffic.

What is the thing that's actually blocking the traffic?

A So in operating system, also some of the network system, you can tell them you know what IP address or what port you want to block.

Q So in Claim 1B, is the filtering subsystem the thing that's doing the blocking?

A No. Like I said, the filtering subsystem in Claim 1B talks about status data. Again, other than the post-filtering residue, you know, if you only focus on security-related events and focusing on the -- only the negative filtering and positive filtering, that's very similar to other security systems such as well-known ones such as firewalls.

The firewalls applying rules is making the decision, and then this separate mechanism that

enforce that decision, for example, say, hey, this IP bad, then the filtering system in the firewall would -- would call an operating system specific function to say, block the traffic if the IP address matched this one. So that's a -- any POSA would understand that's how it -- how these systems are implemented.

Q Okay. So I -- this separate mechanism that you're saying that will enforce the decision, is part of the OS?

A Yes.

Q So when you said in your declaration in IPR2019-01324, at paragraph 17, you said, "the filtering subsystem looks at status data to -- positively filter out what is bad in the traffic."

Is that a true statement or are you changing what you meant by that statement?

MR. GOLDBERG: Objection. Form. Objection scope. Misstates testimony.

A So like I said, you know, this is a true statement because it said in Paragraph 17, right, it says, look at status data to positively filter

out what's bad in the traffic. Essentially, it talks about locate other status data to essentially give decision to say what should be allowed, what should not be allowed in bad traffic. Exactly how you actually block, you know, or how -- how you try to filter out the traffic specifically, any POSA reading this would say, yeah that's not the filtering or rule-matching analysis system is doing.

That filtering subsystem or rule-matching system, it is looking at status data and tells you what should be done, and then what should be done is carried out by separate function that's operating system specific, right?

So I would say there were two, here is basically say that in order to enable this kind of filtering what's bad in traffic. And like I said, a POSA would understand that's carried out by separate function than the rule matching or filtering.

Q I'm handing you what was previously marked as Exhibit 1004. This is the Duvall reference,

the U.S. Patent Number 5,884,033.

A Okay.

Q You're familiar with this reference?

A Yes, I do, yes.

Q Could you turn to Figure 4 of Duvall?

A Yeah.

Q What does the A at the top of that figure mean?

A That A is in reference to the A in Figures 3, that bubble, that circle.

Q So the algorithm that's depicted in Figure 4 actually starts over on Figure 3?

MR. GOLDBERG: Objection. Form.

A Yeah, it further explains what different action would do from -- from Figure 3.

Q So in order to get to the -- the flowchart or the algorithm that's depicted on Figure 4, you would have to first start at Figure 3; is that right?

MR. GOLDBERG: Objection. Form.

A So in Figure 3 it talks about whether this transmission is open or not, it's open, don't

do anything. If it is about to open, then you applied, you know, these decisions. Is it immediate versus deferred, and then further in Figure 4, explain what deferred action means.

Q I don't think that answered my question at all.

MR. GOLDBERG: It did.

Q So the algorithm that's depicted in 4, to get to that portion of the algorithm, you have to start at the algorithm on Figure 3; is that right?

MR. GOLDBERG: Objection. Form. Asked and answered.

A I already answered in the context of a new open connection, because otherwise it will not start with Figure 3 in the first place. And Figure 3, like I said, start with is this connection open or not. If open, don't do anything, just kickback -- keep -- go back and look at the next transmission. And Figure 3 is only applied when a connection or transmission is about to be opened, okay?

Q So --

A And then if -- if the -- if -- if decided that there should be a deferred action, then Figure 4 tells you what that deferred action really is for this -- for this newly opened connection.

Q Okay. So but the first step in Figure 3 is, you start at where it says, "start"; is that right?

A I'm sorry /can you repeat that question?

Q In Figure 3 --

A Yeah.

Q -- the first thing is you start at the start box, right?

A Mm-hmm.

Q So then the first decision is, is the data stream open?

A Mm-hmm.

Q So if it's not open, you go back to the start; is that right?

A No. If it's open, you go back to start. Not open, you -- not open, you proceed.

Q Let's turn to paragraph 110 in your

declaration.

A Okay. Okay.

Q In paragraph 110, you say, "A POSA reading the Schneier claims would have understood that the filtering process that creates post-filtering residue must be distinct from the analysis of post-filtering residue that follows."

A Mm-hmm.

Q What's your basis for that statement?

A So as I said here, right, on the next page, I cited to Figure 2, basically you can think about the data coming from sensor collector, go through negative filtering, goes to positive -- positive filtering and then -- -- and then what's remaining form the post-filtering residue that would be analyzed by the anomaly detection subsystem.

So you can think about the anomaly detection's doing analysis work of the post-filtering residue, but it doesn't itself create the post-filtering residue because it is given the post-filtering residue.

Q The anomaly engine is not actually recited in Element 1B of the claim; is that right?

A So in 1B it talks about an analysis, you know, of post-filtering residue. So I would say Figure 2, anomaly detection subsystem, a POSA would agree that's an example embodiment of analysis of post-filtering residue.

Q My question is a little bit different. The -- the anomaly engine is not positively recited as an element of 1B?

MR. GOLDBERG: Objection. Asked and answered.

A So 1B talks about followed by an analysis of post-filtering residue. I would say any POSA would agree that anomaly -- anomaly analysis subsystem is an analysis.

Q So I get that detail as described in Figure 2 of the -- of the '641 patent. But my question is a little bit different. It is that I'm saying that that limitation is not actually a requirement of Element 1B of the '641 patent?

MR. GOLDBERG: Objection. Asked and

answered.

A Which one is not required?

Q The anomaly engine.

A So.

Q Let me ask it a different way. I guess Claim 1B doesn't specify -- doesn't limit what is doing the analysis of the post-filtering residue?

A So 1B --

MR. GOLDBERG: Objection to form.

A -- talks about an analysis of post-filtering residue. And like I said, a POSA reading that, and you referenced Figure 2, would agree that anomaly event detection subsystem is an analysis. If you say -- if you ask what else can you do, I would say most POSA would -- would throw in anomaly detection. Would say, yeah, I would try anomaly detection. That's a very common sense -- a POSA would say, common sense thing to do.

Q So I -- I guess my question is a little different though. I'm saying I get that that's one way to implement it. One way to implement the

post-filtering analysis of the post-filtering residue is to use an anomaly engine, as disclosed in the '641 patent. I understand that.

But what my question is -- is basically saying is: Do we agree that Claim 1B doesn't limit the analysis of the post-filtering residue to just being done by anomaly engine?

A So like I said, 1B only says, "Followed by an analysis of post-filtering residue." And like I said, a POSA reading this can understand what negative filtering already means allow things that are not interesting, and positive filtering means you focus on the non-interesting things, and you say, okay, what do you do with the post filtering -- filtering residue. I think a POSA would agree that the most -- most obvious or sensical [sic] thing to do is apply anomaly detection. Is anything else? Could be, but to me it's very hard to imagine a POSA would say, I'm not going to do anomaly detection at all. That would be -- yeah, that would be very strange. Like I said, POSA would say, yeah, of course, you

already throw away things that might just -- you already throw away things that are not interesting. You only focus on things that are known to be interesting, okay?

For the remaining, what else can you do? I think anomaly detection would be the first thing that comes to mind to most -- to POSA. A POSA would agree to what I just said.

Q Can we turn to Paragraph 114 of your declaration.

A Yeah.

Q Paragraph 114, the last sentence, you say, "Petitioners' use of deferred action filters as meeting both the filtering and analysis limitations makes clear they are trying to read out limitations in Schneier."

Did I read that correctly?

A You read that correctly.

Q What is your basis for saying that the petitioner is using the deferred action filter for meeting both the filtering and the analysis limitations?

A Okay. Let me read the context here.
(Document review.)
So -- so what we're saying here, I mean I think the whole -- the paragraphs from 110 to 114 essentially is -- essentially saying that the analysis of post-filtering residue should be separate from the process of forming or creating the post-filtering residue. Really what it means that the analysis of post-filtering residue should happen after filtering. And what we're saying here is that the -- the deferred action, action itself is doing filtering, is not doing analysis of things that remains after filtering. It's doing filtering. So because it's doing the filtering, you're not analyzing the post-filtering residue. That's what we say here.
Q So going back to Duvall, would you agree that Figure 3 is showing the -- the steps for applying direct-action filters? Is that a fair characterization of what Figure 3 is showing?
A It talks about if it's not deferred, what direct actions can be -- can be had, like allow a

block, yes. Can mean block or allow.

Q And Figure 4 is showing the steps that would be taken for deferred action filters in Duvall.

Is that a fair characterization?

A It talks about -- it explains deferred action, yeah.

Q Okay. And if you look at the petition, which I just put in front of you with the '641 patent, if you look on Page 29.

A Yeah.

Q There is a subsection, little romanette i, that talks about "Duvall discloses a filtering subsystem coupled to analyze status data, wherein the analysis includes filtering."

Do you see that?

A Mm-hmm.

Q So on pages 29 through 31 of the petition, lays out how Duvall discloses the filtering; is that right? Is that your understanding of what the petition is showing?

A Let me try to refresh my memory here.

I'm sorry, can you repeat your question again?

Q So this subsection of the petition at pages 29 through 31 which talks about Duvall disclosing the filtering, it -- the page -- let me try that again.

You would agree that pages 29 through 31 in this section of the petition is describing how Duvall meets the filtering required by element 1B?

Is that your understanding of what's on pages 29 through 31 of the petition?

MR. GOLDBERG: Objection to form.

BY MR. TUMINARO:

Q Well, how about this, maybe we look at the first paragraph under the subsection on Page 29.

A Okay.

Q The sentence says, "Duvall discloses that its filtering system analyzes status data and that this analysis includes filtering."

Do you see that?

A I see that, yes.

Q It goes on to say, specifically, "Duvall

uses direct-action filters which indicate that the system should unconditionally allow or unconditionally block a transmission."

Do you see that?

A I see that, yeah.

Q So this section is describing how Duvall's direct-action filters meet the filtering limitation of Claim Element 1B.

Do you agree? Is that how you understand the petition?

MR. GOLDBERG: Objection to form.

A I do not agree. No, I don't.

Q Why not?

A I mean, there are multiple elements of 1B. For example, doesn't talk about -- at least the first paragraph on Page 29 does not talk about post-filtering residue, for example.

Q Well --

A That's in 1B.

Q So exactly. If you go to Page 31, the analysis of the post-filtering residue is described in the subsection that's -- that starts

on Page 31. And if you read that section, the petition is -- is mapping, essentially, the algorithm that's shown in Figure 4 of Duvall as analyzing post-filtering residue that's illustrated for example on Page 35.

Is that how you understand the petition?

MR. GOLDBERG: Objection to form.

A So, I mean, I understand that's what the petitioner's expert is saying in his report or declaration, but like I said, I only offered an opinion in my report to say that is not correct because deferred action is doing filtering, not post-filtering analysis.

Q So what I'm confused about is -- the way I understand the mapping in the petition is that the petition is essentially relying on Duvall's Figure 3 and the algorithm disclosed in Duvall's Figure 3 about these direct-action filters to describe how Element 1B, the filtering feature of element 1B is taught. But then Figure 4 of Duvall is used in the algorithm disclosed in Figure 4 for showing how Duvall discloses the analysis of the

post-filtering residue. And it seems like that's -- you do not understand the petition to be doing that.

And is that true?

MR. GOLDBERG: Objection to form.

A I understand what the petitioner's expert was trying to say, but like I said in my report, I think, you know, I disagree with his opinion because my opinion I offered in my report is that deferred action is not -- is not analysis of post-filtering residue. It's actually doing filtering. You cannot do both filtering and post-filtering analysis.

Q So it's your opinion -- I'm just trying to understand what your opinion is when you say this at the bottom of Paragraph 114, that "the deferred action in Duvall is simply filtering and it's not analysis of a post-filtering residue."

Is that what your testimony is?

A Yeah, it's basically doing -- discarding -- doing discarding, which is filtering, you know, by discarding, and so it's

not doing post discarding or post filtering. So that's why it cannot be also doing analysis of post-filtering residue. There's no residue. You basically throw them away.

Q Now, what description does the '641 patent provide about what type of analysis is performed on the post-filtering residue?

A So you already talked about this, right. We say analysis. The 1B says analysis of post-filtering residue, and then Figure 2 give you an embodiment which, like I said, most POSA would say, yeah, makes sense, you do anomaly analysis.

Q But what is the -- I guess my question is, what does the '641 patent say that the anomaly analysis is, what does that entail?

A The POSA would agree that anomaly detection is not something that look like normal. Also it's not known attack, that's what anomaly detection definition.

Q So anomaly detection is some sort of pattern matching?

MR. GOLDBERG: Objection.

Mischaracterizes testimony.

A That's not what I said. There are multiple algorithms that can be used for anomaly detection. There are multiple Ph.D. theses attempting to this that -- in this space.

Again, it's a big field, but in principle a POSA would say, yeah, for things that residue after negative and positive filtering, anomaly detection would make most sense to try first.

Q I guess what I'm confused about, what I don't understand is: What is encompassed within anomaly detection. I don't even know what --

A Say again.

Q I don't understand what is included within anomaly detection.

MR. GOLDBERG: Objection. Form.

A So like I said, a POSA would say anomaly detection means what you detect anomalies. What's anomalies? It doesn't look like normal. Why is it attack? We don't know for sure because if a known good thing would be negative filtered, known bad things would positively filter. What's

remaining makes most sense to apply anomaly detection by definition.

Q What I'm trying to understand and I'm not --

A Yeah.

Q I'm trying not to talk past each other.

I don't understand how would a POSA implement an anomaly detection? I understand you're trying to find something that's anomalous, but how do you find that anomalous thing? What do you do to find the anomalous thing?

A I mean, I can go on forever. Part of the thesis talk about that as well. I mean, in particular, I apply machine learning to basically a ton of normal data, attack data, something in between. Yeah, there's other kind of method that was well-known in the late 1990s. My thesis was from 1999. So by then I publish my thesis work, yeah, most people know that. Even before that, SRI International in the 1980s talked about anomaly detection. It's a well-known piece of technology. A POSA would know, okay?

You can Google it.

Q Can you give me some examples of how you might do that? I know you said it's a broad field, but how might you --

A So, for example, let's say CPU usage. You say normally use ten percent CPU, boom, this time use 90. Is it normal? No, it's not normal. Is it attack? We don't know it's attack. Is anomaly? Yes. You won't detect the anomaly in the first place and then -- and then what do they do? Well, there may be it's worthwhile for you to look further for other stuff. That's the easiest example of anomaly detection. There are many things you can do.

Q Let's talk about status data for a second.

A Okay.

Q Would you agree that status data provides information about the status of a monitored network?

A I think there is some kind of claims construction term. I would love to be able to refer that so that I don't have to contradict.

Let me see. Also cited here in my report. Let me see, maybe the --

(Document review.)

Q If I could offer a suggestion?

A Yeah.

Q In your declaration in the IPR 1324 at paragraph 65 you talk about status data.

A 65? Sorry, which -- which -- oh, you mean the --

Q In IPR-2019-01324.

MR. GOLDBERG: The Fortinet IPR.

MR. TUMINARO: The Fortinet IPR.

MR. GOLDBERG: On Page 29.

BY MR. TUMINARO:

Q Yes. Page 29, paragraph 65, second sentence.

A Again, Page 29.

Q Page 29, paragraph 65.

A I'm sorry, there are two reports. Sometimes it gets confused. All right. Bottom of Page 29, right? Yeah.

Q And if you want to read that to refresh

your memory, that's fine.

MR. GOLDBERG: Anything else you need to read, Wenke to answer the question.

(Document review.)

A Okay. I read that.

Q So would you agree that status data provides information about the status of a monitored network?

A It talks about status data provides information about the status of the network and components.

Q Okay. And the status data may include fields that are extracted from a data packet, right?

A From packets and identification, identification of components involved in a potential event.

MR. GOLDBERG: I'll just object to scope.

BY MR. TUMINARO:

Q One of the fields in a data packet, is that the IP address, right?

A That's one example.

Q Would you agree that an IP address can be an example of status data?

MR. GOLDBERG: Objection. Scope.

A Again, really depends on the context, meaning that status data may have multiple elements. Again, a lot of contextual information. Let's say if you say, oh, this IP address by itself he knows about, no, he actually have no other facts about this IP address. So, again, it's, yeah, I mean, I'm not saying IP is not useful, but like I said, it's one of the, you know -- one of the, sort of -- one of the data elements of status data, but normally for you to say, oh, I have status data that tells me the status -- status of the network, typically you need some information. For example, not just IP, but you also have black list or white list of the IPs. So, anyway.

Q So I just -- we would agree, though, that status -- I mean, an IP address is an example of something that could be status data?

A Yes, again, in security monitoring depends

on the context whether you call this status of the -- in the context of secure monitoring or in the context of lower -- in the context of whether you'd know the IP means you know the status of the network. Like I said, IP by itself doesn't carry enough information. You may need some additional status data to tell you why you think this IP information is useful.

Q So I'm confused by your answer. Are you -- is your testimony that the IP address is not status data?

MR. GOLDBERG: Objection. Mischaracterizes testimony. Scope.

A What I'm trying to say is that the IP address by itself really depends on how you use it. You say, IP, boom, bad, based on what, oh, based on a black list, which means that IP itself is status of data in the context of if you know the black list or white list.

Q Okay.

A You see what I'm saying?

Q Yeah, yes.

Let's go to Claim Element 1C.

Element 1C recites an analyst system.

Do you see that?

A Yes.

Q What is an analyst system?

A Okay. So I think we talk about this in my report as well, but let me see whether there is more specific language in the Schneier patent that talks about analysis system.

(Document review.)

Okay. So it talks about that. Let me see.

Okay. Back to my report.

Yeah, so like I said, in my report, right, so paragraph 122, I basically say a POSA's understanding of the term, "analysis system" will be -- would be informed by Schneier disclosure. For example, Schneier's specification explains how the security analyst trained in network security utilizes an analysis system such as the closed SOCRATES, S-O-C-R-A-T-E-S, system to resolve potential incidents that are identified in Claim

Limitation 1B. So then, basically, it goes -- I reference the Schneier patent Column 3, line 41 to 50. Yeah. So...

Q And the Claim Element 1C says that there is a communication system that transmits information about the identified events to the analyst system, right?

A Says, "a communications systems coupled to transmit information about the identified events to -- to an analysis system associated with the security monitoring system."

Q Does the -- do the claims specify the type of connection that is required between the communication system and the analyst system for transmitting the information?

A Let me see here.

MR. GOLDBERG: Objection. Scope.

A Okay. So in the -- first of all, the Schneier patent '641 talks about the gateway system. Okay. So the gateway system essentially connects linking basically the probes system on the customer side to a SOC, a security center,

security operational center.

So that's from an architecture point of view. And then I think further down it talks about, so -- talks about the -- let me see here -- yeah, so the gateway system, if you look at the Figure 1, communicates with the probe using Pipes.

Then further on in the patent it talks about the Pipes, I think starting basically Column 5, line 50 to all the way to Column 7, Line 10, it talks about using -- essentially, establishing a secure transmission. You talk about VPN, SSL, TOS. Essentially, any POSA reading this would say, yeah, it basically means, you know, the communication between the probe and the SOC is secure.

Q So I appreciate that the '641 patent itself and the detailed description has details about how the information is transmitted. I'm not asking about the spec, the detailed description. I'm asking about the claims.

My question is: Did the claims specify the type of connection that is required to

transmit the information to the analyst system?

MR. GOLDBERG: Asked and answered. Scope.

A So like I said, Claim '641 talks about the embodiments and gives detailed example in the figure explanation. If it's not sufficient, I'm going to say that a POSA, in particular working security, would be shocked to learn that the communication between the customer side and your SOC is not over secure communication. They would be -- that would be, like, capital crime you're committing.

Q So you understand that in a patent you could have a detailed description that has a lot of details, but the claims don't necessarily need to include all of the details that are described in the detailed description? Do you understand that?

A I understand that, but, like I said, POSA reading this would just immediately know, a communication, we talk about security and secured operations, you don't send data that has anything to do with the customer side over Internet on an

insecure channel. That's like completely crazy. My point is that you don't have to -- I mean, again, even though it's not -- does not explicitly say you shall encrypt, you shall use TRS -- in the claim language, but like I said, a POSA reading this would say, yeah, of course, why do you encrypt? The standard answer from POSA would say, why not?

Q I guess my question is a little bit different. I guess what I'm asking you is, in order to meet the limitations of these claims, like Claim Element 1C, whether for infringement or for invalidity, does the transmission need to be encrypted? Does the claim say one way or the other?

MR. GOLDBERG: Objection. Scope. Form.

A So like I said, I think a POSA reading the patent already gets the teaching from the patent through the figures and explanation, and, like I said, a POSA reading this would say, yeah, of course I will encrypt.

Q Did the claims require a specific way for

implementing the analyst system? Not the detailed description, but the claims themselves.

A I'm sorry, and -- and to --

Q Do the claims themselves include any specific requirements for how to implement the analyst system?

MR. GOLDBERG: Objection. Scope.

A Let me see.

So I mean, I think there are multiple claims that talks about analyst system, analysis system.

It talks about, for example, let's say claim -- yeah, for example, Claim 6, right, it talks about the multi-stage analysis includes analysis at both a probe and analysis at the secure operation center. So that tells you the operation -- the secure operation center performs multi-stage analysis. And then as another example, it talks about -- let's see, let's say Claim 10, right, talks about, you know, the secure operations center to perform further computer-based analysis, right, and then Claim 11

talks about the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis, and so on. So actually, like I said, multiple claims talks about the analysis system.

Q Can we go to Page 58?

A What.

Q Page 58 of your declaration. Paragraph 126.

A Okay.

Q The first sentence you say, "I would also note that the petitioner and its experts' rationale for including an analyst in the first place seems to be based on obviousness in light of references other than Duvall and Chu."

Do you see that?

A I see that.

Q You'd agree that those other references constitute evidence of the state of the art, right?

MR. GOLDBERG: Objection to form.

A But like I said, the next sentence, but

none of those other cited references show that transmitting to an analyst system would be inherent to Duvall and Chu.

Q So we'll get to that next sentence in a minute, but, first, could you answer my question that -- my question was: You would agree that those other references constitute evidence of the state of the art, right?

MR. GOLDBERG: Objection to form. Asked and answered. Scope.

A So, okay. Let me see. This is not mine.

So, again, I mean, I need to look at the references to refresh my memory to comment on your question.

Q Would you agree that prior -- that other references would provide context for how a POSA would interpret Duvall and Chu, for example?

MR. GOLDBERG: Objection to form.

A Again, depending on the exact references, I cannot recall the details of those references. I mean, you can share with me, I can take a look, and then opine on them -- on those.

Q One of the references that we looked at earlier was Exhibit 1037.

A 1037. All right. Okay, yeah, sure. Yeah.

Q And in Exhibit 1037, we looked at, for example, the IBM NetRanger product and outsourced security monitoring and the Realsecure outsourced security monitoring.

Do you recall us talking about that earlier?

A We -- I recall discussing NetRanger and Realsecure in the context of remote monitoring.

Q And would you agree that a reference, for example, like Exhibit 1037 would constitute evidence of the state of the art?

MR. GOLDBERG: Objection to form.

A Again, I mean, I think 1037 is not enough detail of what a NetRanger would be doing in the IBM emergency response center to -- to compare that with what the claims of '641 -- '641 is talking about. For example, '641 talks about all this analysis, you know, aggregating,

synthesizing, presenting alerts on ensemble basis. Those examples that I -- I do not see in the -- in Exhibit 1037. So I cannot comment on that, whether they are state of the art or not.

Q So you can't comment on whether Exhibit 1037 provides -- constitutes evidence of the state of the art? You don't know one way or the other?

MR. GOLDBERG: Objection. Asked and answered. Form.

A So like I said, I need a more detailed description of what they do at their -- at their -- essentially, their version of security operations center. It's just not enough details to tell me what kind of analysis they're doing for me to say, oh, that's the state of the art even in reference to the '641. Just like I said, not enough detail for me to comment on that.

Q Would you agree that the other references, like, for example, Exhibit 1037, provide context for how a person of ordinary skill in the art would interpret Duvall and Chu's disclosures?

MR. GOLDBERG: Objection to form.
A Can you repeat the question again?
Q Would you agree the other references, like, for example, Exhibit 1037, provide context for how a person of ordinary skill in the art would interpret Duvall and Chu?
A No. I think we went through this, right? I think Duvall, a POSA would say that's not what security monitoring is about. Chu is also not. So for a POSA to say, oh, I read Duvall and Chu, then let me, you know -- pair them up -- pair them up, and also in NetRanger. That's very far fetching. Like I said to begin with, a POSA would not look at Duvall and Chu to say, oh, that teaches me something about security monitoring, because they are not. So then the POSA would say, oh, I can improve upon them for security monitoring with all these other allegedly state of the art.
Q So it's your opinion that Exhibit 1037 does not provide evidence of the state of the art?
MR. GOLDBERG: Objection.

Mischaracterizes testimony.

A So I think I already said that I need more -- more detailed description of what they do in their version of the security -- security operations center to opine that whether what they're offering is -- is state of the art with respect to what the limitation of -- of '641 patent. There's nothing to compare.

Q I'm sorry. I --

A There is nothing to compare, because there is not enough details about NetRanger or Realsecure for me to say that's -- that they are state of the art.

Q You go on, the second sentence in paragraph 126 you say what the other references show that none of the other references -- let me start over.

"None of the other cited references show that transmitting to an analyst should -- would be inherent to Duvall, Chu."

Do you see that?

A Yes.

Q Why did you use the word "inherent" in paragraph 126?

A Okay. So -- so I would refer you back to about the previous page, I think paragraph 124, right? In particular, yeah, basically, last sentence of 124 says, "At best petitioner's expert seems to argue why it would have been obvious to have an analyst manage Duvall, Chu system, but there is no explanation of what that means, you know, what system those analysts would be using or, you know, why is it inherently you need an analyst.

Q Yeah, so I get it in paragraph 124 you say one thing, but in 126, you italicize the word inherent. So, obviously, you thought it was important that -- to use that word.

So why did you use the word inherent in paragraph 126?

MR. GOLDBERG: Objection. Form.

A So inherent means you have to have it. So, basically, the petitioner's expert didn't say why did they -- you know, why it's necessary for

Duvall and Chu to need an analyst or analysis system and what they do, where they come from, none of that. So that's why, yeah, it's not -- that's why a POSA would say, ah, what, Duvall and Chu -- first of all, they're not related to security, now you say, they have analyst and the analysis system would be using an IBM Realsecure. It's like -- what I'm trying to say here is that the -- Duvall and Chu, I mean, the petitioner's expert did not say why they need analysis system to begin with. So why would you as a POSA say, okay -- like I said, POSA would -- would already disagree that Duvall and Chu had anything to do with security monitoring.

Secondly, a POSA would say, oh, also then why do you want to include all of these allegedly state-of-the-art to have -- to have an analysis system -- to analysis system. These things just don't add up to POSA.

Q Well, you would agree with me that it was known to have remote security monitoring services like the ones that are described in Exhibit 1037

that we talked about earlier today?

A So I think we discussed this earlier, right. So I think for NetRanger, it talks about -- yeah, I -- basically, I wouldn't -- like I said, there is not enough detail to say that's a managed security services like what the '641 patent is teaching. It essentially talks about having experts, security experts remotely to manage your -- sensors on your network. That's all. It's very different from what '641 is teaching. So that's why I would say that Realsecure, as this Exhibit 1037 is -- is describing, tells me that NetRanger is doing remote monitoring. And that's, like I said, again, that's very different from managed security services like '641.

Q What does -- what does managed security service require?

MR. GOLDBERG: Objection to form.

A So in a context of '641, it talks about you have -- you have, like Figure 1, it talks about, you know, you have probes or sensors on

customer's side and it passes on information about security events to your remote analysis system that performs through the analysis, provides, you know, information or update and then, like I said, '641, some of the claims -- like I said, Claim 6 -- Claim 10, Claim 11, so on, so forth, talks about some of the details of the analysis system in terms of what it is doing.

So based on that, I could not opine on what NetRanger and Realsecure are doing because they do not provide details of what they -- and how they operate.

Q Okay. So you would agree with me, you said this in paragraph 60 of your declaration and IPR in the Fortinet IPR, that remote monitoring services were known.

You would agree with me, right?

A Let me see. Yeah, the last sentence I say in paragraph 60, I say, "remote -- remote monitoring services were known, but not common, and there was no well-considered architecture to run them to help discover unknown intrusions."

Q And the IBM NetRanger and the Realsecure as disclosed in Exhibit 1037 are examples of remote monitoring services, right?

MR. GOLDBERG: Objection. Scope.

A Yeah, they are remote monitoring services, but, really, the context of paragraph 60 is also -- just look at the paragraph 61, I talk about '641 patents, describes an entirely -- entirely novel architecture for the remote monitoring network for intrusion, right? So really I emphasize entirely novel.

So that's what I'm trying to say is that with respect to '641, this architecture, all these other allegedly state of the art, does not give enough detail for me to say they are state of the art with respect to '641.

MR. GOLDBERG: Jonathan, when you finish this line of questioning, we'll take a break.

BY MR. TUMINARO:

Q Just, we agree that the IBM NetRanger and Realsecure in Exhibit 1037 examples of remote monitoring services and the Realsecure has a

central console as shown on Page 278 of Exhibit 1037, right?

MR. GOLDBERG: Objection. Form. Scope. Mischaracterizes prior testimony.

A Yeah, so it talks about Realsecure supports remote sensing stations called engines that report to a central console.

Q And that central console would be displayed on a computer system, for example?

MR. GOLDBERG: Objection. Scope.

A Again, does not give the details, but console, yeah, console has to be on some sort of electronics stuff, yes.

Q And a security expert, for example, from X-Force team could look at information on that console, correct?

MR. GOLDBERG: Objection. Form. Scope.

A So, again, I think I went through this. Like I said, without detailed description of the Realsecure's operations and different teams doing what, I could not comment on that. Like I said, based on the paragraph on Page 279, it only talks

about the X-Force team, you know, do their own research and use their connection with the underground world, so on and so forth. It didn't talk about the X-Force team looking at the central console. The console of the -- yeah, it didn't talk about look at the central console.

Q So this is the last question, then we can take a break.

A Yeah.

Q My question is: Would it be beyond the level of ordinary skill in the art for a person to realize, based on this disclosure in Exhibit 1037, that a member -- a security expert of the X-Force team could sit in front of that console and look at data? Would that -- would that be beyond the skill of a person of ordinary skill in the art?

MR. GOLDBERG: Objection. Scope. Asked and answered.

A So, again, my experience with secure operation center is that it's actually a lot of nuances depending on how you want to operate. And sometimes it's a conflict of interest. You know,

one analyst would be looking at one customer data and the same analyst cannot look at another customer's data that they're in the same industry competing. There's a lot of nuances. That's one thing.

Second thing is -- my point is not obvious -- hey, the data is on the information -- on the console. Everybody take a look. It's more nuanced than that.

Second thing is, you know, Realsecure, as I understand, or ISS at the time and now it's called IBM, I don't know ISS maybe. Is -- all these are large operations so my point is they have multiple teams doing different things and one team may hand data off to another team. And X-Force, like I said, as described in this paragraph, really this paragraph emphasizing the X-Force ability to do new research looking -- you know, looking at underground data. That literally I would say they are further away from the information on the central console. That's all I can say, really based on the information provided

to me.

MR. GOLDBERG: Let's break.

MR. TUMINARO: We can take a break.

(Recess.)

BY MR. TUMINARO:

Q Welcome back, Dr. Lee. Dr. Lee, I'd like to turn to paragraph 143 of your declaration.

A 143.

Q In the first sentence, you say -- I'm sorry -- 143 in the '889, this IPR proceeding. It's on Page 67.

A 67. Okay. 143.

Q 143?

A All right.

Q The very first sentence in that paragraph you say, "The only analysis petitioner suggests would be performed by Duvall-Chu's purported analyst system occurs after the identifying step is already complete."

Do you see that?

A Yes.

Q In support of that statement, you cite to

the petition at Section 6A5.

Do you see that?

A Mm-hmm.

Q If you look over at the petition at the table of contents. At 6A5, that relates to Claim 4.

A Okay.

Q Do you see that?

A Let me see, but -- okay. So let me see, Claim 4 --

Q And maybe I'll help you out. You can turn to Page 44 of the petition.

A Mm-hmm, yeah.

Q So at Page 44, that's where the petition talks about Claim 6.

Do you see that?

A Page 44. Yeah, it talks about Claim 6, yes.

Q Do you see at the bottom of the page on Page 44 there is a sentence that starts with "the Duvall-Chu combination teaches."

Do you see that sentence?

A Yeah.

Q I'll read it for the record, "The Duvall-Chu combination teaches analysis at a probe followed by analysis at an analyst system."

Do you see that?

A Yes.

Q "And then as support for the analysis at the probe, the petition points to Section 6A2C."

Do you see that?

A Mm-hmm.

Q "And then for" -- going to the next page, Page 45 -- "for analysis at the analyst system, the petition points to Section 6A2D."

Do you see that?

A Mm-hmm.

Q And my question is, do you express an opinion in your declaration about whether Section 6A2C discloses analysis at the probe as required by Claim 6?

A Let me look at this more carefully. Okay? So you're talking about what the petition is talking about, you are reading the petitioner

expert's declaration, the Page 44, right?

Q Page 44. So I was looking at -- at your declaration in Section I, paragraphs 142, 143, and 144. You're talking about Claim 6, right, and you're offering your opinion about why Claim 6 is supposedly not met, right?

A Let me -- let me see, okay. 143, okay, is within the context of talking about Claim 6, okay? So I'm referring to the petition expert's declaration Page 44, it talks about Claim 6. Okay. I'm with you now. Okay.

Q And the only specific section of the petition that you cite in paragraph 143 is Section 6A5, right?

A 6A5, yeah, maybe that was -- that was -- that should be 6A7 instead. Okay. Whatever, that's a typo, I would say.

Q And looking at the petition at Section 6A7, as I pointed out, the petition is saying that the analysis at the probe is described in Section 6A2C.

Do you see that at the bottom of Page 44?

A Yes, that -- so yes, 6 -- 6A2C is, again, still the -- still within the petitioner's expert report, right?

Q Yes.

A Okay.

Q And my question is: Do you offer any opinion anywhere in your declaration about whether Section 6A2C discloses analysis at the probe as required by Claim 6?

A Okay. Let me take a closer look to refresh my memory. Okay. Okay let me see and go through here.

(Document review.)

Okay. So I already forgot your question. Can you repeat it again?

Q Do you offer an opinion anywhere in your declaration about whether Section 6A2C discloses analysis at the probe as required by Claim 6?

A So the way I read Claim 6 is that it furthers Claim 2, right? So Claim 6 says, "The system of Claim 2, wherein the multistage analysis includes analysis at the probe and analysis at a

secure operation center is configured to receive data from the probe."

And yeah, so, basically, Claim 6 explained what multistage analysis should include, and that's part of the identifying step. So let me see whether the petitioner talks about multistage analysis in 6A2C.

Q And I could help you out. Look at the bottom of Page 44, the petition, where it says, "The Duvall-Chu combination teaches analysis at a probe followed by analysis at an analyst system."

And in support of that statement, the petition cites two other sections, Section 6A2C and Section A2D.

Do you see that?

A Yes. So I'm --

Q Maybe I'll just shortcut.

A Okay.

Q In your paragraph 143, 144, and actually 142, you don't provide any analysis of Section 6A2C or Section 6A2D; is that correct?

A Hold on.

So like I said, the way I read Claim 6 is explained -- first of all, I think Claim 2 talks about the identifying step in 1B essentially should include performing multistage analysis. And then Claim 6 further to say the multistage analysis include analysis at the probe and analysis in the secure operations center. So the point is that the analysis we're talking about is part of identifying, not after identifying. I think that's what we said here in paragraphs 142 to 144 to say that petitioner never talks about analysis as being part of the identifying step. It only talks about after the identifying step. So that -- and that's why it doesn't meet the requirements of Claim 6.

Q Again, I just don't -- your paragraphs 142, 143, and 144 don't provide any analysis of Section 6A2C or Section 6A2D of the petition; is that a correct statement?

MR. GOLDBERG: Objection to form. Asked and answered.

A So I already talked about in 143, I point to paragraph 44, 46, even though I cited probably the wrong section heading, but -- but it's clear that, you know, 44 and 46 talks about Claim 6 in the petition expert's report. So my opinion here stands that the petition expert's opinion in 44 -- on page -- pages 44 to 46 talks about the analysis, but that's after the identifying step, whereas Claim 6 requires that the multistage analysis at the probe and at the security operations center is part of the identifying step.

Q Okay. Can we go to Paragraph 217.

A 217?

Q Of your declaration?

A 217. All right.

Q Paragraph 217, I think it's the third sentence. It says, "The inventors recognized that information."

Do you see that?

A Mm-hmm.

Q I'll read it for the record. "The inventors recognize that information regarding

unknown security threats likely resided within the post-filtering residue left over after filtering performed at the probe (i.e., the sentry of Counterpane MSM).

Do you see that?

A Yes.

Q But you didn't show in your declaration that Counterpane's MSM includes positive filters, negative filters, and residue data that is neither positively nor negatively filtered as required by Element 1B of the '641 patent?

MR. GOLDBERG: Objection to form.

BY MR. TUMINARO:

Q Did you?

A I'm a little confused by your question. Can you repeat again?

Q You haven't shown that Counterpane's MSM includes positive filters, negative filters, and residue data that is neither positively filtered nor negatively filtered as required by the claims of the '641 patent, for example, Element 1B?

A Okay. Let me take a look.

(Document review.)

Okay. So if -- let me see -- so like I said, you know, I think we went over this before, in Paragraph 213, the last sentence, I did say that Counterpane MSM is an embodiment of the Schneier patent and is captured by the claims, right.

Then I further talk about, for example filtering, I talk about -- let's say, Paragraph 214, I talk about "the sentries collect data from network devices and utilize over 20,000 filters to filter potential security threats."

So I think -- like I said, I think as I said multiple times today, that a POSA would say, okay, what do you mean? What are you filtering? A POSA would say, first of all, you throw away things that you don't -- that you don't think is interesting, that's negative filtering. Then you focus on things that you think are likely to attack, that's positive filtering. And then what's remaining, what do you do? That's the invention of '641.

So, basically, it talks about, okay, the post-filtering residue should also be analyzed. So like I said, my point is, by reading my report and understanding what MSM is doing, having all of this filtering, a POSA will agree, yeah, of course it performs negative filtering and positive filtering. I would say that any security monitoring system would do that already. It is -- it is the analysis of post-filtering residue that's a novelty to me. That's novelty in 1B, and also, of course, all this analysis I'm talking about is based on residue on status data. That's pretty -- that's I would say very well -- kind of unique as well.

Q So in your opinion, the sentries collecting data from a network device and utilizing over 20,000 filters to filter potential security threats teaches a POSA the limitations of Element 1B?

MR. GOLDBERG: Objection. Misstates -- mischaracterizes prior testimony.

A So that sentence talks about -- teaches a

POSA about negative filtering and positive filtering. Like I said, any POSA reading that sentence would say, yes, of course, what do you do? The answer, hey, what do you think those filters are doing? I think the reaction from POSA would say negative filtering throw away things that you don't think is interesting or useful to a security analysis or something that you just permit. Positive filtering, looking at things that potentially bad, that you know are potentially bad. And the very next sentence talks about the sentry also utilizes an analysis engine to further analyze post-filtering residue, which is sent -- which is then sent to the SOC and SOCRATES. Like I said, that's the novelty of the '641 patent and that, by the way, that sentence is also part of Claim 1B, right? 1B talks about not just negative filtering and positive filtering, but also talks about analysis of post-filtering residue.

Q So to be clear, the evidence that you're relying on to say that Counterpane MSM meets

Element 1B is Exhibit 2009 at Page 6 and Page 12 as you cited in Paragraph 214 of your declaration; is that right?

A I think we went through this earlier today. I also say, in addition to Page 12, I also offer to say -- yeah, Page 15 talks about sentry. So talks about there are so many filters, what they do, kind of thing. So my point is, yeah, I mean, people, a POSA would understand it teaches, you know -- teaches 1B. Further, and then also let me see here, yeah, and then other pages, for example, 116 talks about correlation and trending. And yeah, so -- so like I said, this document has information that you rely on to draw the conclusion that MSM meets the claim limitation because it also talks about what you do with the managed security monitoring and so on and so forth.

Q Okay. Can we go to Paragraph 218 of your declaration?

A Yeah.

Q First sentence says, "Likewise, although

theoretically possible with human analysts, prior art systems could not actually utilize human analysts to monitor such data for threats due to the sheer volume of the residue data."

Do you see that?

A Yes.

Q But human analysis of monitor data was actually available in the prior art, wasn't it?

A Can you repeat the question again?

Q Human analysis of monitored data was actually available in the prior art, wasn't it?

MR. GOLDBERG: Objection to form.

A Again, depends on what data that you're talking about. What data, what are you referring to as data?

Q Information about potentially security-related events in traffic on a client's network is data that was analyzed by humans in prior art systems, right?

A I don't know which prior art system you specifically referring to.

Q IBM provided such a service for human

analysts to analyze information from clients' networks, right?

MR. GOLDBERG: Objection. Scope.

A That's -- that's not how I remember. It talks about -- I say on Page 277 of Exhibit 1037, right, it talks about -- you know, the paragraph talks about when an event is detected, IBM security experts are -- notify you and help you respond to the event. So I would say that in this paragraph, what it says is that the human analyst or security expert is looking at the event or reports of the event. That's different from, let's say, you know, the raw packet data from the network.

Q And ISS Realsecure also provided a service for human analysts to analyze data from a client's network.

MR. GOLDBERG: Is that a question?

A So, again, like I said, at the bottom of 277 of Exhibit 1037, it talks about, like, NetRanger, Realsecure supports remote sensing stations called engines that report to central

console. I think I went through this multiple times today's that a POSA would understand that the engines will send reports or event -- about events to the central console but not the, I would say, the raw data from your organization. You know, multiple reasons, including volume of data, including security or privacy concern and so on.

Q I'm not talking about the raw data. I'm talking about the information -- the -- the information would be about the potentially security-related event?

MR. GOLDBERG: Objection scope. Form.

A So, again, I wish the -- these reference -- the referenced -- related work would talk about most explicitly what, you know, what's the format of the report and so on. But, yeah, in general, you want to -- you want to send -- I mean, like, as Claim C is talking about, right, you transmit information about the identified events to analyst system, not the raw data.

Q Let's go to Paragraph 219.

A Okay.

Q In Paragraph 219 you say, "Indeed, when Counterpane MSM entered this space with its new approach to managed security monitoring, its competitors were mainly IDS monitoring companies that performed discrete filtering functions and did not have the level of detection monitoring and response that were provided by Counterpane MSM."

Do you see that?

A Mm-hmm.

Q Who were the competitors that you were referring to? And to help you I'll give you Exhibit 210 that you cite.

MR. GOLDBERG: Thank you.

A All right.

Yeah, so in this reference, right, we talk about -- talk about page number -- Page 3, on Page 3, it talks about, "Until now, according to analysts the market for such network monitoring services has remained largely in the military and large corporate data processing markets and has been dominated by companies like IBM, Electronic Data Systems, and Computer Sciences Corp. Yeah.

And then the next paragraph talks about new entrances besides Counterpane Internet Security Systems and Pilot Network Services. Yeah. So I think the point is that still relatively -- compared with today, today we have so many vendors. Back then it was still a relatively smaller number compared with today.

Q So would IBM be one of the competitors that you were referring to in Paragraph 219 of your declaration?

A Yeah, I would say IBM was a mainstay. I mean they, you know, they acquired -- acquired NetRanger in the mid 1990s as I remember. But again, like I said, they are one of the main -- main -- main companies, at least back then.

Q And one of the features that you say in Paragraph 219 that distinguishes Counterpane MSM from its competitors was the level of detection, monitoring, and response provided by Counterpane MSM.

Do you stand by that statement?

A Yes.

Q The claims don't specify a required level of detection, do they?

A Which claim are you talking about?

Q The claims of the '641 patent. None of the claims of the '641 patent require a specified level of detection, do they?

MR. GOLDBERG: Objection to form. Scope.

A So I think there's multiple limitations here, talks about multistage analysis. That's, you know, Claim -- Claim 6, right, and then Claim 11 -- 11 talks about aggregating, synthesizing, presenting alerts on ensemble basis, you know, and also Claim 13 -- well, Claim 12 talks about correlation. Claim 13 talks about frequency, and so on and so forth. Basically, all these claims are actually -- really set the '641 apart from discrete filtering.

Discrete filtering means, okay, event A, I detected it. Event B I detected it. But correlation means, hey, even A and B are correlated. So you just report the fact that these -- actually it's the same event. Whatever.

So -- so that's what I'm trying to say is that -- that's what Paragraph 219 is referring to.

Q But the claims that you talk about, you talk about the type of analysis that might be done, but do the claims specify a required level of detection that has to be met by a system?

MR. GOLDBERG: Objection. Scope.

A What do you mean by level of detection?

Q You used the word level of detection in Paragraph 219.

A Okay.

Q And I'm trying to understand whether the claims don't require a specified level of detection.

A Okay. I see what you're saying. Okay.

So 219 talk about did not have the level of detection, monitoring, and response that were provided by Counterpane. A POSA would say, what do you mean by security? You detect attacks by monitoring what's going on, and you respond to attacks, meaning that detection monitoring and response, these are the essential elements of

security -- security functions that you want to have, detection, monitoring, and response.

Q So that's my --

MR. GOLDBERG: Are you finished, Wenke?

THE WITNESS: Yeah.

A So what I'm trying to say is all this limitation talks about that, and that the patent from the architecture Figure 1, Figure 2, and all these claim languages talks about identifying analysis. So those are -- essentially covers detection and monitoring, and then the -- you know, giving feedback and modifying, that's part of response. So that's what sets '641 patent apart from the -- from the art.

Q What you're saying in Paragraph 219 is the features that set Counterpane apart from its competitors are the level of detection, the level of monitoring, and the level of response.

Where do the claims require a level of detection?

MR. GOLDBERG: Objection. You are misreading the paragraph.

A So essentially I talk about does not have the level of detection and monitoring and response that were provided by Counterpane MSM, meaning that compared with Counterpane MSM, they're not on the same level, I mean.

Q I get that. I get that Counterpane's product, in your opinion, had better detection or like the level of detection of the Counterpane's product, the level of monitoring of Counterpane's product and the level of response of Counterpane's product distinguished its from its competitors. I get that. But my question is, where are those distinguishing features in the claims of the '641 patent?

A Okay.

MR. GOLDBERG: Objection to form.

A So I think I said earlier, in Paragraph 213, that Counterpane MSM is an embodiment of the Schneier patent and is captured by the claims. So that's a question, yeah, the claims talks about essentially the technology that enables the level of detection monitoring and

response of -- provided by Counterpane MSM.

Q Which claim language specifies the level of detection that distinguished Counterpane from its competitors?

A So like I said, you know, again, the context is with respect to other competitors doing only discrete-filtering function. So I would say that -- let's say post-filtering analysis of post-filtering residue, that's a new thing. That's meaning that, okay, after you decide allow, not allow, there's still more things to be done. That's basically brings the detection at a different level already, okay?

And then talks about transmitting information to the analyst system, again performing more analysis, more monitoring. And then you receive feedback, you update system. Again, that's response. And by the way, you also further to provides, you know, it -- so there are further claims that talks about the identifying, meaning that the detection monitoring involves multistage analysis, that includes correlation,

you know, aggregating, synthesizing, you know, counting frequencies, and so on and so forth. It's all there, it's all in the claims. You talk about the different level of detection monitoring and response provided by Counterpane MSM.

Q How do you know that the Counterpane MSM had a level of detection monitoring and response that distinguished it from its competitors if you don't remember how IBM's NetRanger product actually worked?

A I know of NetRanger that's one of the older systems, from what we know, and based on what I read in this Exhibit 1037, yeah, I basically, I think my opinion in the report is -- stands, meaning that IBM does not provide the same level of detection monitoring and response as provided by Counterpane. There is no evidence that IBM does that they provided that level of detection monitoring and response.

Q How do you know that the Counterpane MSM provided a better level of detection, monitoring, response than its competitors if you never used

the Counterpane MSM and you never have seen it used?

MR. GOLDBERG: Objection. Form.

A Okay. So like I said, my report is based on references. So I cited references of Counterpane MSM as described by its inventor, yeah, so that's -- that's my -- that's how I draw my conclusion.

Q So your conclusion that Counterpane MSM had a better level of detection monitoring response than its competitors is based on Exhibit 210?

MR. GOLDBERG: Objection. Misstates the testimony.

A That's one of the references I cited in my report. Yeah. And also, like I said, I'm a POSA, I know the development of the technologies at the time or the history before that, so I'm just confident with my -- with my opinion described in the report.

Q How can you know that the level of detection monitoring response of the Counterpane

MSM is better than its competitors if you hadn't measured the performance of Counterpane versus the performance of its competitors?

MR. GOLDBERG: Objection. Asked and answered.

A So like I said, I would say in Paragraph 213 that Counterpane is an embodiment of the Schneier patent, and also it's captured by the claims. And like I said, multiple times, these claims are basically novel -- novel way of doing detection monitoring, in particular doing analysis of post-filtering residue, and the analysis is based -- is on status data. And like I said, you know, there is a transmission of security-related information, information related or about the identified events to analysis system in this case would be the security operation center to do further analysis. And the further analysis include, for example, in correlation, aggregation, and so on and so forth. That was not obvious from what I knew about other systems back then.

Then also talks about giving feedback,

updating the -- the probe and so on. So, again, it really covers detection monitoring and response on a level that I did not see from -- from other work. I mean, unless you give me a document to take a closer look, but, yeah, based on documents that I have, that's my opinion.

Q Let's turn to Page 104.

A Okay.

Q And at the bottom of the Page 104, you have a header -- a heading to a subsection about industry praise and commercial success of the Counterpane MSM.

Do you see that?

A Yes.

Q And that section spans, I guess, from Paragraph 223 to paragraph 227; is that right?

A Yes. Mm-hmm.

Q Do you show anywhere in these paragraphs that the so-called industry praise or commercial success of the Counterpane MSM is due to its ability to positively filter data, negatively filter data, and retain that data that is neither

positively nor negatively filtered?

MR. GOLDBERG: Objection to form.

A Okay. So -- so I think in both paragraphs 223 and paragraph 224, right, I talk about, you know, different recognitions and praises, specifically mention Counterpane's. For example, in -- I mean, the keyword here is managed security monitoring that really, you know, essentially that's what's being -- that's what Counterpane is being praised about is about the security monitoring services or managed security monitoring. And like I said, you know, throughout the today's discussion, that we say what does Counterpane do in terms of monitoring. I think I answered this multiple times, that essentially just practiced the claims of the '641 patent because, like I said, you know, MSM is an embodiment of the Schneier patent and it's captured by its claims. So that's what its monitoring is doing. And it's being praised. That means the technology that it practices according to the claims is being praised.

Q But where, like, what words could you point to in any of these paragraphs that's showing that the so-called industry praise or commercial success of the Counterpane's MSM is due to its ability to positively filter data, negatively filter data, and retain data that is neither positively nor negatively filtered?

MR. GOLDBERG: Objection to form. Asked and answered.

Q Can you point to any words in the paragraphs that show that?

A So I would say that, you know, these praises, right, they -- I mean, if you give me the reference, I can take a closer look again.

On the other hand, it's like some of these praises, they would say, hey, I give you award of X, you know, and X is a collection of technology that you use according, let's say, to the patent.

So what I'm trying to say here is Counterpane is being praised, let's say, for managed security monitoring and you say exactly what? That has been explained by the -- by the

reference that the -- we have discussed from, you know, reference exhibit -- I don't remember the number, but Bruce Schneier wrote this article about Counterpane and managed security monitoring. So my point is that also explain what managed security monitoring really means for Counterpane. And like I said, Counterpane MSM is embodiment of the Schneier patent. It captures the -- the claims.

So, again, if people pay -- people praise Counterpane managed security monitoring, they basically praise this whole system, I mean, yeah. Does it have to mention specific features? I don't know why it's necessary.

Q So you don't think it would be necessary for the commercial success of the industry praise to be due to any of the claim's features?

MR. GOLDBERG: Objection to form. Misstates testimony.

A That's not what I said. I said that it's well understood by the writing from Bruce Schneier, the inventor, surrounding discussion

that Counterpane MSM is an embodiment of the '641 patent, and it captures these claims. So really meaning that when you ask, hey, what do you mean by managed security monitoring from Counterpane MSM? Well, I'm going to be recite all these -- all these claims. And so my point is that when Counterpane's managed security monitoring is being praised, essentially they're praising these claims. That's all, that's all -- that's my opinion.

Q Okay. Can you point to any words in the paragraphs 223 to 227 that show that the so-called industry praise or commercial success of the Counterpane MSM is due to its ability to dynamically modify the analysis capability of the probes?

MR. GOLDBERG: Objection. Form.

A So like I said, all these praises, right, from industry are talking about Counterpane's industry-leading security monitoring service or managed security monitoring. That's exactly what that means. Like I said, Schneier talks about

the -- in its article and then, like I said, it actually -- Counterpane MSM is an embodiment of the patent. I mean, I can go through line by line and tell you those are the features that have been implemented in Counterpane MSM. So Counterpane MSM is being praised, essentially they are praising the -- praising the claims -- praising the claim elements of the patent. To the extent that they did not, you know, single out or cite specific claim doesn't mean they are not praising all claims. That's all I can say.

Q Okay. Can you turn to paragraph 13, Page 5 of your declaration.

A Okay. Page 5. Okay.

Q You say that, "I have been asked to assume that a person of ordinary skill in the art pertaining to Schneier at the time it was invented has the education and experience that petitioner's expert has set out in his declaration."

Do you see that?

A Yes.

Q So you're not disputing petitioner's

experts' description of what a person of ordinary skill in the art would be, are you?

A Let me see.

I've been asked to assume that. So I did not -- did not dispute, okay. Yeah.

Q So you're not disputing it?

A I asked -- I was asked to assume. So I assumed it.

MR. TUMINARO: We can take a quick break.

MR. GOLDBERG: Mm-hmm.

(Recess.)

BY MR. TUMINARO:

Q Welcome back, Dr. Lee.

A Thank you.

Q Dr. Lee, I want to go back to Duvall and confirm that I understand your testimony.

A Okay. Yeah, okay.

Q Duvall Figure 3, I think what you said is in the decision step at Step 100, if it's -- if it's open, you go back to the start. If it's not open you proceed.

Is that the way you understand this

figure?

A Yes, that's how I refer to -- I would refer you to column 4, line 37. It says, "Referring to Figure 3, the filtering system can filter outgoing messages on the basis of the IP address of the host server that's being contacted by the client. The filtering system detects when a -- when the client opens the data stream for -- a particular IP, a particular port, and IP address, Step 100.

So really that means Step 100 is being triggered when the client is trying to open the data stream, which means that data stream has been opened, means go back and wait for the next time the client tries to open a stream. That's how I read it.

Q So if it's closed, then you proceed down through Figure 3?

A What do you mean closed?

Q If the data stream is closed or it's not open, you would proceed?

A It's about to open, basically that's what

the language is saying here. If it's closed, there is nothing you need to do. Closed, what do you do? Nothing to monitor about. This transmission is already over. You don't do anything about the transmission already.

So really what I'm trying to say is that if the transmission -- I mean, figure -- Step 100 according to the spec here in Column 4 is essentially you -- essentially Step 100 detects when the client opens the data stream for a particular port and IP address.

Q And would you agree that the only way that you can get to, sort of, A is if you go through Step 100, Step 102, and Step 104 and you determine at Step 104 that no immediate action is required?

MR. GOLDBERG: Objection. Form.

A So -- so if further down on -- on -- in Column 4 and starting in Line 65, it says, "If at Step 104 it is determined that no immediate action must be taken, it is determined whether a deferred action must be taken with respect to any of the achieved filter" -- filter, yes, that's that 116,

yeah.

Q So the way that you get to A is you -- you start at start and go through Box 100, 102, 104 and you potentially go to the deferred option to get to A; is that right?

MR. GOLDBERG: Objection to form. Asked and answered. Mischaracterizes testimony.

A So like I said, if 104 tells you that no immediate action must be taken, then you say, is it then, should you go to defer or not? If yes, then you go to A.

Q And A is -- the beginning of the analysis at A starts at the top of Figure 4, right?

A That's my understanding, yes, that's correct.

MR. GOLDBERG: Objection to form.

MR. TUMINARO: I have no more questions.

MR. GOLDBERG: No questions. We're done.

(Time Noted: 4:46 P.M.)

ACKNOWLEDGMENT OF DEPONENT

I, WENKE LEE, PH.D., do hereby acknowledge that I have read and examined the foregoing testimony and the same is a true, correct, and complete transcription of the testimony given by me and any corrections appear on the attached errata sheet signed by me.

_____ _____

(SIGNATURE) (DATE)

CERTIFICATE OF SHORTHAND REPORTER-NOTARY PUBLIC

I, ANITA M. TROMBETTA, RMR, CRR, Notary Public within and for the State of New York do hereby certify:

That WENKE LEE, PH.D., the witness whose deposition is hereinbefore set forth, was duly sworn by me before the commencement of such deposition and that such deposition was taken before me and is a true record of the testimony given by such witness.

I further certify that the adverse party, BT AMERICAS INC., was represented by counsel at the deposition.

I further certify that the deposition of WENKE LEE, PH.D., occurred at the offices of Proskauer Rose LLP, Eleven Times Square, New York, NY 10036-8299 on Thursday, April 4, 2024, commencing at 8:58 A.M. to 4:46 P.M.

I further certify that I am not related to any of the parties to this action by blood or marriage, I am not employed by or an attorney to any of the parties to this action, and that I am in no way interested, financially or otherwise, in the outcome

of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my notarial seal this 8th day of April, 2024.

My commission expires: 10.07.2025



ANITA M. TROMBETTA, RMR, CRR

A
a2d
264:15
ability
131:13, 151:6, 258:18, 285:21, 287:5, 289:14
abirnet
53:11
able
58:16, 76:10, 130:2, 132:4, 133:13, 134:10, 145:21, 151:16, 160:16, 234:21
absolutely
43:10, 45:2, 91:10, 91:15, 193:20, 198:15
accept
151:18, 151:19
accepts
152:2, 155:17
access
138:9, 138:19, 142:15, 143:18, 144:6, 145:7, 145:9, 147:13, 152:16, 155:5, 158:17, 163:18, 164:5, 164:19, 167:5, 167:22, 168:17, 191:7, 192:5, 192:17, 193:3
accessing
153:10
accomplish
107:13
according
8:13, 15:20, 15:21, 64:7, 121:21, 122:1, 190:2, 209:19, 275:17, 286:22, 287:18, 293:8
account
58:10, 139:10, 140:1, 140:15
accurate
92:7, 205:2
achieved
293:22
acknowledge
295:2
acknowledgment
295:1
acquire
143:7, 143:10, 143:11, 143:13, 154:20
acquired
148:21, 276:12
act
210:2
action
195:21, 195:22, 196:2, 217:15, 218:4, 219:2, 219:3, 224:13, 224:20, 225:11, 226:3, 226:7, 229:12, 230:10, 230:17, 293:15, 293:19, 293:21, 294:9, 296:19, 296:21
actions
193:15, 225:22
activated
103:5
activities
184:16
actual
158:4, 158:6, 177:6, 180:5, 211:4
actually
14:4, 28:11, 29:5, 29:16, 29:19, 37:15, 39:2, 48:8, 60:7, 63:13, 75:16, 88:1, 109:5, 109:16, 129:9, 156:16, 163:9, 180:2, 183:11, 184:17, 188:3, 213:4, 214:7, 216:5, 217:12, 221:1, 221:20, 230:11, 237:8, 245:3, 257:20, 264:20, 272:2, 272:8, 272:11, 277:16, 277:22, 282:10, 290:2
adaptive
38:10, 38:18, 41:8, 43:20, 158:2
add
6:3, 6:7, 63:14, 137:18, 252:19
addition
271:5
additional
13:20, 150:9, 195:5, 195:9, 238:6
address
192:3, 192:18, 192:19, 212:15, 212:16, 212:19, 212:20, 212:21, 214:11, 215:5, 236:21, 237:1, 237:7, 237:9, 237:20, 238:10, 238:15, 292:6, 292:10, 293:11
adjust
66:3, 66:9, 66:20, 70:13, 72:6, 84:12, 84:13, 86:20
admin
83:9
adverse
296:10
affect
154:10, 154:11
affected
156:11
affixed
297:3
after
12:9, 15:14, 125:14, 165:1, 198:6, 208:19, 225:10, 225:13, 232:8, 259:18, 265:10, 265:14, 266:8, 267:2, 281:10
afterwards
78:11
agencies
71:2
agent
77:13
aggregate
163:6, 165:16
aggregating
245:2, 247:22, 277:11, 282:1
aggregation
284:19
agree
15:15, 40:22, 43:15, 50:6, 53:14, 56:14, 59:18, 60:4, 74:18, 74:19, 80:14, 83:22, 86:5, 92:19, 118:13, 125:10, 156:7, 172:4, 177:17, 184:10, 200:17, 200:18, 200:22, 201:4, 203:3, 203:7, 208:16, 209:9, 221:6, 221:15, 222:13, 223:5, 223:16, 224:8, 225:17, 227:7, 228:9, 228:12, 231:16, 234:17, 236:6, 237:1,

237:19, 245:18, 246:6, 246:15, 247:13, 248:19, 249:3, 252:20, 254:13, 254:17, 255:20, 269:5, 293:12
agreement
75:2
ah
252:4
ahead
77:20, 169:16, 169:21, 170:1, 172:13, 185:21
air
40:15
alert
63:15
alerts
62:9, 62:10, 63:14, 245:2, 248:1, 277:12
algorithm
217:11, 217:17, 218:8, 218:9, 218:10, 229:3, 229:17, 229:21
algorithms
232:3
aligned
88:2
alive
143:17, 144:5, 144:6
allegedly
249:18, 252:16, 255:14
allow
139:11, 149:11, 156:5, 187:2, 189:22, 207:3, 223:11, 225:22, 226:1, 228:2, 281:10, 281:11
allowed
36:2, 190:5, 190:6, 216:4
allowing
142:13, 192:17
allows
150:12
almost
50:8, 147:6, 147:9, 147:19, 150:15, 153:13
along
52:7
already
16:15, 20:5, 20:7, 20:17, 21:21, 22:16, 23:6, 23:14, 24:5, 31:18, 34:2, 34:8, 40:7, 40:19, 42:21, 44:20, 65:14, 73:22, 97:16, 104:10, 119:2, 120:18, 121:4, 129:1, 132:6, 132:12, 148:21, 169:22, 171:16, 179:3, 209:17, 218:13, 223:11, 224:1, 224:2, 231:8, 243:18, 250:2, 252:12, 259:19, 263:14, 266:1, 269:8, 281:13, 293:4, 293:5
also
6:11, 17:13, 23:14, 24:17, 25:18, 26:22, 27:11, 32:5, 37:1, 37:11, 42:2, 55:8, 55:15, 58:13, 60:9, 61:10, 66:1, 74:7, 74:19, 80:19, 92:11, 97:1, 110:9, 110:17, 125:15, 136:10, 153:13, 162:19, 203:17, 214:9, 231:2, 231:18, 235:1, 237:17, 245:11, 249:9, 249:12, 252:15, 255:7, 269:2, 269:11, 270:12, 270:17, 270:19, 271:5, 271:10, 271:16, 273:15, 277:13, 281:18, 283:16, 284:8, 284:22, 288:5
alternatively
158:3
although
271:22
alto
1:4
always
42:12, 50:8, 70:9, 71:5, 78:1, 78:2, 125:19, 142:13, 147:15
americas
1:9, 296:11
among
182:3
amount
39:14
analogy
147:19
analysis"
115:10
analyst
12:12, 13:7, 14:8, 15:16, 16:4, 16:6, 16:11, 16:13, 16:18, 16:20, 17:2, 17:16, 61:21, 67:4, 75:11, 76:8, 76:9, 77:4, 77:14, 77:16, 78:1, 78:3, 79:18, 80:5, 82:16, 93:18, 95:19, 239:2, 239:5, 239:19, 240:7, 240:14, 242:1, 244:1, 244:6, 244:10, 245:13, 246:2, 250:19, 251:8, 251:12, 252:1, 252:6, 258:1, 258:2, 259:18, 261:4, 261:12, 264:11, 273:10, 274:20, 281:15
analysts
45:6, 52:9, 59:20, 60:3, 61:13, 66:7, 70:6, 73:13, 73:15, 74:12, 75:9, 75:10, 79:22, 80:15, 251:10, 272:1, 272:3, 273:1, 273:16, 275:18
analyze
9:13, 28:1, 28:4, 29:1, 35:8, 37:2, 37:12, 40:10, 42:3, 52:9, 59:20, 60:4, 61:13, 61:21, 62:11, 63:6, 63:19, 65:7, 66:7, 66:18, 71:9, 71:12, 82:21, 89:10, 89:19, 99:12, 104:12, 105:4, 107:3, 187:4, 194:2, 200:21, 201:5, 201:19, 226:14, 270:13, 273:1, 273:16
analyzed
86:15, 104:20,

105:8, 105:12, 105:16, 220:16, 269:2, 272:18
analyzes
176:13, 200:18, 227:18
analyzing
64:20, 86:9, 87:3, 88:17, 90:11, 200:3, 200:4, 200:5, 202:13, 203:10, 225:15, 229:4
anita
1:22, 2:11, 296:2, 297:10
anomalies
232:18, 232:19
anomalous
45:1, 233:9, 233:10, 233:11
anomaly
40:13, 40:19, 43:3, 44:20, 115:10, 194:18, 195:2, 195:4, 220:16, 220:18, 221:1, 221:5, 221:9, 221:15, 222:3, 222:13, 222:16, 222:17, 223:2, 223:7, 223:17, 223:20, 224:6, 231:12, 231:14, 231:16, 231:18, 231:20, 232:3, 232:8, 232:12, 232:15, 232:17, 233:1, 233:8, 233:21, 234:9, 234:13
another
11:19, 14:1, 48:19, 73:8, 89:1, 139:5, 139:9, 144:14, 177:13, 183:17, 200:5, 211:16, 244:18, 258:2, 258:15
answer
14:3, 15:6, 15:10, 17:13, 25:5, 29:18, 49:9, 73:5, 93:3, 93:8, 93:9, 114:14, 131:14, 160:22, 170:6, 184:14, 197:4, 198:5, 198:8, 198:10, 198:13, 202:20, 207:1, 207:2, 207:16, 209:18, 236:3, 238:9, 243:7, 246:5, 270:4
answered
7:19, 14:10, 16:22, 19:9, 20:4, 21:10, 21:20, 22:15, 23:5, 23:13, 23:14, 26:13, 26:14, 26:17, 32:3, 72:9, 81:7, 81:15, 86:22, 88:21, 90:14, 91:7, 91:8, 91:14, 91:15, 101:8, 118:2, 120:17, 120:18, 124:15, 125:17, 130:6, 131:17, 132:6, 134:8, 136:8, 142:2, 148:17, 191:18, 197:16, 199:12, 209:16, 210:14, 212:10, 212:11, 218:5, 218:12, 218:13, 221:12, 222:1, 242:2, 246:10, 248:10, 257:18, 265:22, 284:5, 286:15, 287:9, 294:7
answering
15:5, 25:1, 91:2, 161:4, 196:16, 196:18, 198:15, 206:16
answers
8:6, 50:19
antispam
46:16
antivirus
46:16
any
27:2, 28:5, 29:22, 42:11, 44:5, 45:2, 59:14, 73:7, 78:8, 86:5, 89:5, 92:2, 98:10, 108:20, 117:17, 123:15, 124:16, 124:18, 128:12, 128:14, 133:7, 134:6, 134:9, 137:2, 140:18, 141:16, 159:14, 163:15, 163:20, 164:9, 164:14, 171:9, 173:20, 180:5, 198:11, 207:16, 208:12, 210:3, 211:8, 215:5, 216:7, 221:14, 241:12, 244:4, 263:6, 264:21, 265:18, 269:7, 270:2, 287:2, 287:10, 288:17, 289:11, 293:21, 295:6, 296:19, 296:20
anybody
129:20
anyone
102:11, 136:16
anything
5:22, 71:4, 79:17, 82:11, 83:8, 84:22, 85:19, 87:12, 87:13, 97:22, 99:18, 102:4, 105:3, 105:6, 105:14, 105:18, 119:8, 123:1, 124:7, 124:8, 149:1, 173:15, 178:3, 178:12, 179:7, 186:10, 187:19, 195:19, 218:1, 218:18, 223:18, 236:2, 242:21, 252:13, 293:5
anyway
48:1, 70:11, 102:5, 111:15, 127:17, 147:21, 156:11, 165:12, 165:14, 168:5, 237:18
anywhere
30:5, 186:10, 263:7, 263:16, 285:18
apart
277:17, 279:14, 279:16
appeal
1:2
appear
295:6
appears
170:20, 170:21
appliances
46:13, 47:17
application
134:22, 138:6, 138:12, 139:6, 144:3, 145:1, 145:3, 145:8, 145:21, 146:2, 146:10, 146:21, 147:7, 147:11, 147:20, 148:11,

148:12, 151:9, 153:20, 155:8, 167:5, 167:6, 167:8, 174:13
applications
145:11, 149:15, 152:14, 152:18
applied
162:12, 172:1, 172:8, 172:17, 173:11, 193:15, 218:2, 218:20
applies
172:5
apply
7:10, 145:5, 162:1, 162:15, 162:21, 163:14, 165:13, 166:12, 167:14, 169:14, 169:21, 172:13, 185:8, 193:21, 198:1, 223:17, 233:1, 233:14
applying
162:4, 163:12, 169:6, 170:19, 171:7, 172:12, 172:22, 173:1, 174:5, 211:4, 211:5, 214:21, 225:19
appreciate
14:2, 95:2, 241:16
approach
275:3
april
1:15, 296:16, 297:4
architecture
39:19, 43:11, 55:16, 56:6, 59:5, 60:22, 61:3, 99:9, 241:2, 254:21, 255:9, 255:13, 279:8
area
58:8, 60:12, 64:18
argue
153:12, 251:7
argument
72:17, 73:4, 196:15, 198:21
argumentative
20:11, 21:2, 32:3, 69:7, 83:1, 83:6, 84:15, 85:15, 86:11, 88:20, 120:7, 148:17, 158:10, 159:18, 197:6, 197:11, 198:10
around
29:7, 40:12
art
38:22, 40:2, 42:12, 49:5, 49:15, 64:2, 64:15, 66:17, 115:22, 117:10, 156:19, 175:21, 245:19, 246:8, 247:15, 248:4, 248:7, 248:16, 248:21, 249:5, 249:19, 249:21, 250:6, 250:13, 255:14, 255:16, 257:11, 257:16, 272:2, 272:8, 272:11, 272:19, 272:20, 279:14, 290:16, 291:2
article
184:6, 288:3, 290:1
asked
7:18, 14:10, 16:21, 19:9, 20:3, 21:9, 21:19, 22:14, 23:4, 23:13, 26:3, 26:12, 32:3, 68:10, 72:8, 81:6, 81:14, 83:4, 88:21, 90:14, 91:7, 101:7, 118:3, 120:16, 124:14, 125:16, 130:5, 131:16, 136:7, 142:1, 148:17, 191:17, 197:19, 197:21, 198:4, 199:11, 206:9, 209:15, 210:13, 212:9, 218:11, 221:11, 221:22, 242:2, 246:9, 248:9, 257:17, 265:21, 284:4, 287:8, 290:15, 291:4, 291:7, 294:6
asking
7:14, 7:16, 7:21, 8:1, 10:14, 10:15, 23:10, 26:6, 26:19, 60:18, 61:9, 64:1, 64:14, 75:5, 81:3, 83:3, 85:10, 87:1, 88:11, 88:15, 89:16, 90:6, 90:7, 91:3, 91:4, 120:12, 120:13, 120:21, 122:6, 122:9, 123:10, 123:21, 131:9, 133:5, 134:4, 134:5, 136:2, 136:3, 136:4, 148:15, 152:22, 187:17, 197:9, 197:15, 241:19, 241:20, 243:10
aspects
34:5
assess
105:5
assigned
58:10
associated
13:2, 13:13, 213:11, 240:10
association
184:21
assume
175:21, 204:21, 290:15, 291:4, 291:7
assumed
291:8
assumption
175:4, 175:5
attached
295:6
attack
40:15, 40:16, 76:11, 77:10, 86:10, 87:5, 88:19, 89:11, 89:20, 90:12, 93:20, 231:18, 232:20, 233:15, 234:8, 268:20
attacked
40:9, 77:9
attacker
50:5, 50:10
attacks
42:17, 46:18, 66:3, 66:8, 66:19, 70:13, 70:20, 71:4, 71:5, 72:6, 72:7, 72:12, 84:11, 84:12, 85:4, 85:5, 85:13, 85:16, 86:4, 86:20, 112:9, 135:14, 278:19, 278:21
attempting
232:5
attended
29:15

attorney
296:20
attractive
58:15
automatically
138:11
available
29:2, 58:13, 130:13, 131:11, 132:3, 133:6, 133:21, 140:5, 151:6, 272:8, 272:11
ave
3:6
avoid
182:22
award
287:16
aware
28:10, 134:9, 136:9, 136:10, 136:16
away
42:13, 42:14, 44:6, 44:13, 110:2, 141:1, 194:15, 203:12, 224:1, 224:2, 231:4, 258:20, 268:16, 270:6
awesome
44:9, 184:8

B

back
12:10, 21:11, 51:6, 57:6, 67:15, 75:19, 106:3, 141:14, 141:21, 143:17, 143:21, 151:1, 162:20, 195:20, 196:7, 212:2, 218:18, 219:18, 219:20, 225:17, 239:13, 251:3, 259:6, 276:6, 276:15, 284:21, 291:13, 291:15, 291:20, 292:14
bad
42:18, 44:18, 44:22, 149:22, 150:13, 184:4, 184:5, 184:16, 184:20, 185:1, 185:20, 186:11, 187:21, 203:5, 203:22, 205:15, 206:1, 208:5, 208:9, 208:10, 210:8, 210:17, 211:9, 213:8, 215:2, 215:15, 216:1, 216:4, 216:17, 232:22, 238:16, 270:10, 270:11
bank
42:13, 140:10, 140:15, 151:10, 151:14
based
15:22, 29:2, 41:10, 45:17, 70:5, 84:13, 87:9, 89:9, 89:14, 89:16, 89:17, 89:18, 90:17, 91:19, 92:10, 92:16, 102:13, 104:5, 105:1, 105:2, 105:17, 116:4, 140:11, 142:7, 184:20, 193:3, 238:16, 238:17, 245:14, 254:9, 256:22, 257:12, 258:22, 269:12, 282:12, 283:4, 283:11, 284:13, 285:5
basic
111:22, 116:20, 119:1, 138:22, 139:2, 140:17
basically
8:19, 13:16, 17:14, 22:21, 24:13, 24:18, 24:20, 26:21, 27:8, 28:10, 31:1, 31:4, 38:5, 38:6, 39:3, 39:13, 40:3, 40:13, 41:1, 41:21, 47:14, 59:6, 59:14, 60:6, 68:8, 74:5, 76:18, 80:8, 97:16, 99:12, 100:6, 107:19, 119:9, 128:4, 132:18, 137:5, 138:18, 140:14, 142:4, 142:10, 145:10, 150:5, 150:6, 155:1, 155:9, 159:1, 160:2, 160:21, 163:4, 164:21, 164:22, 165:12, 167:4, 167:9, 168:14, 176:8, 177:14, 179:20, 186:22, 196:3, 198:18, 201:5, 210:1, 211:5, 211:10, 216:16, 220:11, 223:4, 230:20, 231:4, 233:14, 239:15, 240:1, 240:21, 241:8, 241:13, 251:5, 251:21, 253:4, 264:3, 269:1, 277:15, 281:12, 282:14, 284:10, 288:12, 292:22
basis
220:9, 224:19, 245:3, 248:1, 277:12, 292:5
because
17:5, 20:21, 29:18, 37:18, 40:8, 47:11, 50:4, 58:16, 62:10, 64:11, 70:22, 73:21, 77:21, 82:20, 96:20, 97:22, 98:13, 111:10, 116:22, 121:11, 129:11, 129:12, 132:17, 139:5, 147:12, 147:17, 148:21, 151:12, 154:11, 155:15, 156:5, 156:12, 156:21, 160:8, 161:4, 164:14, 164:17, 180:10, 180:21, 181:1, 181:7, 182:4, 182:9, 182:22, 183:9, 184:8, 185:19, 187:13, 187:22, 188:13, 191:6, 192:8, 193:4, 193:14, 203:9, 206:9, 215:21, 218:14, 220:21, 225:14, 229:12, 230:9, 232:20, 249:16, 250:10, 254:10, 271:16, 286:17
become
58:14
becomes
150:10, 155:18
been
5:3, 14:20, 26:17, 31:18, 37:20, 41:11, 45:20, 48:13, 48:15, 54:1, 85:11, 102:17,

150:14, 160:6, 172:5, 195:8, 202:21, 251:7, 275:21, 287:22, 290:4, 290:15, 291:4, 292:13
before
1:2, 2:11, 6:18, 15:4, 27:21, 28:2, 30:12, 44:5, 52:4, 52:19, 99:18, 122:11, 125:12, 126:11, 143:6, 144:12, 149:1, 151:3, 154:1, 155:21, 212:4, 212:11, 213:1, 233:19, 268:3, 283:18, 296:7, 296:8
begin
104:15, 249:13, 252:11
beginning
42:9, 196:5, 294:12
begins
103:6
behalf
3:2, 3:10
behind
28:16, 33:10, 111:20
being
8:14, 83:6, 83:11, 85:2, 102:6, 109:4, 109:7, 122:5, 123:12, 126:20, 128:21, 129:3, 130:21, 132:4, 133:22, 134:7, 140:6, 145:8, 147:12, 148:5, 149:8, 152:13, 152:18, 152:19, 153:21, 153:22, 155:7, 155:8, 162:10, 162:11, 163:22, 164:22, 167:8, 167:9, 167:15, 167:22, 170:5, 172:7, 172:15, 172:16, 172:19, 173:3, 173:10, 194:16, 194:18, 198:9, 223:7, 265:13, 286:9, 286:10, 286:20, 286:22, 287:20, 289:7, 290:6, 292:6, 292:11
believe
12:1, 12:2, 18:11, 18:20, 19:6, 19:15, 21:5, 23:2, 31:21, 190:12, 191:12
belongs
147:20, 170:8
besides
48:19, 112:15, 276:2
best
44:18, 53:2, 251:6
better
280:7, 282:21, 283:10, 284:1
between
8:12, 13:21, 146:18, 180:6, 233:16, 240:13, 241:14, 242:8
beyond
43:7, 257:10, 257:15
big
69:10, 82:5, 132:12, 165:8, 166:3, 166:9, 169:2, 186:5, 232:6
bigger
167:1, 167:11
bingo
110:7
bit
146:9, 221:8, 221:19, 243:9
black
125:3, 125:8, 237:17, 238:17, 238:19
blanket
137:1
block
3:4, 35:22, 36:8, 36:13, 42:19, 44:9, 91:14, 183:3, 183:8, 183:15, 183:18, 184:3, 187:2, 187:9, 188:1, 188:2, 188:12, 190:17, 190:18, 190:21, 191:7, 191:10, 191:15, 192:3, 192:21, 193:3, 209:7, 211:11, 213:11, 213:13, 213:18, 214:5, 214:11, 215:4, 216:5, 226:1, 228:3
blocked
188:13
blocking
184:10, 184:15, 191:21, 192:5, 192:11, 192:17, 214:2, 214:7, 214:13
blood
296:19
blow
96:10
board
1:2
book
52:16
boom
234:6, 238:16
both
41:1, 114:3, 162:16, 172:22, 174:4, 213:5, 224:14, 224:21, 230:12, 244:15, 286:3
bottom
54:11, 83:18, 230:16, 235:20, 260:19, 262:22, 264:9, 273:19, 285:9
box
195:18, 219:13, 294:3
branch
151:14
branches
151:16
breadth
39:6
break
51:2, 74:9, 102:19, 105:22, 150:17, 150:19, 151:3, 154:2, 211:14, 211:20, 212:4, 212:11, 213:2, 255:18, 257:8, 259:2, 259:3, 291:9
bringing
143:17
brings
159:21, 281:12
broad
39:10, 136:12, 192:15, 234:3
broader
39:11
browser
184:1
bruce
29:14, 288:3, 288:21

bt
1:9, 296:11
bubble
217:10
bucks
139:8, 139:9, 139:10, 139:19, 140:1, 140:3, 141:6
buffer
161:21, 162:4, 162:18
buffering
161:20
build
114:17
building
101:10
bunch
38:19, 68:8, 73:9, 109:22
business
55:21
buy
50:15, 50:16, 50:19, 60:13
bypass
50:12

C

call
24:16, 38:18, 112:14, 142:7, 145:17, 195:18, 213:12, 215:3, 238:1
called
5:3, 44:14, 48:9, 65:18, 67:16, 79:15, 123:13, 137:17, 138:12, 142:10, 161:20, 189:19, 256:6, 258:12, 273:22
calling
64:7, 182:1, 213:17
can't
52:13, 87:14, 97:21, 112:8, 123:15, 128:15, 145:9, 147:12, 167:14, 170:9, 171:14, 172:8, 248:5
cannot
11:14, 42:9, 71:2, 76:16, 90:4, 90:16, 91:19, 94:20, 102:2, 105:15, 105:19, 128:13, 129:12, 130:10, 131:6, 132:19, 135:19, 137:1, 138:21, 139:10, 139:11, 162:15, 163:11, 163:13, 164:5, 164:19, 165:11, 170:7, 170:11, 172:17, 172:22, 173:10, 173:15, 174:4, 186:12, 187:22, 230:12, 231:2, 246:20, 248:3, 258:2
capabilities
48:5
capability
15:17, 45:16, 47:4, 70:4, 132:4, 133:22, 134:7, 165:4, 171:11, 289:15
capable
38:6, 192:11
capital
242:10
capture
23:18, 39:8
captured
19:13, 19:20, 20:6, 20:17, 21:14, 22:1, 22:4, 22:6, 22:17, 23:1, 23:16, 23:21, 23:22, 25:21, 26:3, 26:16, 30:20, 31:6, 31:15, 31:19, 34:8, 36:19, 41:1, 268:6, 280:19, 284:8, 286:19
captures
21:17, 24:4, 39:7, 39:21, 288:8, 289:2
capturing
22:22
card
182:17
care
40:8, 81:22, 83:12, 100:6
career
150:2
carefully
261:20
cares
149:5
carried
216:13, 216:18
carries
24:20, 25:19, 27:12
carry
238:5
case
1:6, 84:17, 96:18, 137:9, 151:18, 284:16
cases
46:12
catch
135:14, 175:16
cause
211:9, 211:10
censor
9:4
censors
39:16, 68:14
center
8:11, 8:17, 58:1, 58:5, 58:9, 58:17, 59:12, 74:5, 74:18, 94:5, 94:17, 97:11, 98:1, 98:6, 240:22, 241:1, 244:16, 244:17, 244:21, 247:19, 248:14, 250:5, 257:20, 264:1, 265:8, 266:11, 284:17
centers
38:15, 97:2
central
65:18, 67:21, 68:5, 68:16, 68:18, 69:6, 77:8, 79:16, 83:21, 84:2, 84:4, 84:22, 85:20, 87:14, 94:17, 95:14, 95:15, 96:14, 97:10, 99:20, 100:1, 100:2, 100:6, 100:8, 100:15, 100:18, 101:2, 101:12, 101:13, 101:17, 101:19, 101:21, 101:22, 102:3, 102:11, 102:15, 256:1, 256:7, 256:8, 257:4, 257:6, 258:21, 273:22, 274:4
centuries
36:20
certain
17:7, 17:8, 21:12, 42:7, 42:8, 42:11, 183:3, 190:17
certificate
296:1

certify
296:4, 296:10, 296:13, 296:18
chaff
45:7
chain
94:5, 94:6
challenge
158:18
challenging
155:18, 156:2, 156:21, 157:3, 157:7, 157:21, 158:7
chance
25:5
change
5:22
changed
172:7
changes
46:14, 46:21, 47:1, 47:6, 47:8, 47:10, 47:14, 47:15, 47:20, 48:3, 48:21, 171:6
changing
215:17
channel
243:1
characterization
225:20, 226:5
characterized
11:5
characterizing
12:3
charge
182:4
chart
94:13
charts
90:3
choose
103:11
chu
124:20, 125:1, 126:8, 245:15, 246:3, 246:17, 249:6, 249:9, 249:10, 249:14, 250:20, 251:8, 252:1, 252:5, 252:9, 252:13
chu's
248:22
circle
217:10
circumstantial
180:14
cite
29:4, 29:22, 30:5, 37:18, 37:21, 259:22, 262:13, 275:12, 290:9
cited
29:5, 29:19, 30:10, 92:17, 220:11, 235:1, 246:1, 250:18, 266:2, 271:2, 283:5, 283:15
cites
264:14
citing
52:11, 89:3
city
101:9
claim's
288:17
claimed
205:13
claims
19:14, 19:20, 20:7, 20:12, 20:16, 20:18, 21:4, 21:6, 21:15, 22:1, 22:5, 22:7, 22:8, 22:12, 22:17, 23:1, 23:9, 23:16, 23:22, 25:22, 26:3, 26:16, 30:20, 31:6, 31:15, 32:1, 34:6, 36:19, 106:6, 175:10, 175:13, 176:1, 193:13, 199:5, 220:4, 234:20, 240:12, 241:20, 241:21, 242:14, 243:11, 243:22, 244:2, 244:4, 244:10, 245:4, 247:20, 254:5, 267:20, 268:6, 277:1, 277:4, 277:5, 277:16, 278:3, 278:5, 278:13, 279:19, 280:13, 280:20, 280:21, 281:20, 282:3, 284:9, 284:10, 286:16, 286:19, 286:22, 288:9, 289:2, 289:6, 289:9, 290:7, 290:11
clarified
200:16
clarify
49:7
clarifying
49:10
clear
10:15, 20:19, 20:21, 22:4, 23:20, 36:8, 104:9, 117:17, 120:1, 121:4, 121:8, 122:5, 138:20, 170:2, 170:15, 173:16, 199:19, 200:15, 212:6, 224:15, 266:3, 270:21
clearer
24:1
clearly
22:16, 71:3, 182:2, 194:10
client
8:8, 78:15, 93:21, 100:9, 152:4, 152:8, 153:1, 153:2, 153:5, 153:16, 154:6, 154:14, 154:16, 155:5, 158:19, 292:7, 292:8, 292:12, 292:15, 293:10
client's
61:14, 61:22, 63:6, 64:20, 66:8, 66:19, 68:1, 68:12, 94:1, 97:13, 98:5, 272:17, 273:16
clients
71:12, 73:12, 151:7, 151:20, 152:2, 152:6, 152:7, 153:3, 153:4, 153:9, 154:6, 154:16, 155:17, 156:15, 158:17, 158:20, 160:13, 273:1
closed
239:20, 292:17, 292:19, 292:20, 293:1, 293:2
closer
263:10, 285:5, 287:14
cloud
59:16
collect
9:1, 9:4, 34:11, 35:2, 36:20, 41:7, 41:20, 59:19, 60:3, 66:18, 67:22, 72:14, 75:7, 76:3, 76:6, 76:17, 99:6, 99:13,

161:11, 162:3, 162:15, 162:18, 163:11, 163:13, 186:22, 268:10
collected
73:14, 78:15, 93:18, 93:22, 98:4, 104:6, 108:11, 161:20, 162:2, 170:5
collecting
160:18, 161:9, 161:14, 161:16, 269:16
collection
287:17
collector
194:13, 220:12
collects
38:10, 75:14, 194:13
column
108:9, 108:10, 109:10, 110:13, 111:3, 112:10, 114:9, 115:6, 117:12, 117:13, 118:4, 119:19, 157:17, 158:14, 188:21, 240:2, 241:9, 292:3, 293:8, 293:18
combination
260:21, 261:3, 264:10
come
50:6, 67:9, 70:15, 71:20, 71:22, 72:3, 84:18, 85:16, 87:21, 186:16, 252:2
comes
42:12, 116:7, 117:18, 169:13, 224:7
coming
75:17, 109:21, 119:7, 159:4, 212:21, 220:12
command
137:13, 141:4, 141:9, 141:12, 141:13, 141:20, 183:10, 183:11, 183:15
commencement
296:7
commencing
296:16
comment
90:4, 94:20, 132:19, 155:22, 246:13, 248:3, 248:5, 248:18, 256:21
commercial
285:11, 285:19, 287:3, 288:16, 289:13
commercially
130:13, 131:11, 132:3, 133:6, 133:20, 151:5
commission
297:5
commit
138:16, 139:4
committing
242:11
common
50:20, 50:21, 55:11, 55:15, 57:5, 60:22, 81:2, 100:17, 209:8, 213:4, 222:17, 222:18, 254:20
communicates
241:6
communication
12:21, 13:11, 13:21, 240:5, 240:14, 241:14, 242:8, 242:9, 242:20
communications
14:12, 240:8
companies
57:2, 57:7, 275:4, 275:21, 276:15
company
47:13, 47:18, 48:16, 48:19, 50:16, 73:7, 73:8, 94:8, 101:10
compare
27:13, 196:4, 196:5, 196:8, 247:19, 250:8, 250:10
compared
276:5, 276:7, 280:4
competency
58:17
competing
258:4
competitors
275:4, 275:10, 276:8, 276:18, 279:17, 280:11, 281:4, 281:6, 282:8, 282:22, 283:11, 284:1, 284:3
complements
65:16
complete
182:8, 204:22, 259:19, 295:5
completely
60:15, 63:21, 85:3, 95:20, 100:11, 101:12, 118:13, 126:8, 153:14, 164:5, 164:21, 182:11, 182:20, 188:6, 188:14, 243:1
complex
135:22, 136:13, 136:22
component
9:5
components
236:11, 236:16
compromise
50:11
compromised
183:22, 184:2
computer
7:4, 24:15, 25:17, 27:10, 101:11, 132:18, 138:3, 140:18, 141:1, 161:19, 162:22, 170:7, 176:7, 178:3, 256:9, 275:22
computer-based
244:22, 245:1
concept
29:8, 29:9, 101:21, 106:12, 111:22, 112:22, 113:13, 113:17, 113:19, 114:18, 115:1, 116:15, 119:1, 121:11, 121:15, 121:21, 122:1, 122:9, 122:11, 123:4, 123:7, 123:10, 123:12, 123:13, 124:1, 124:3, 124:10, 124:12, 125:2, 125:11, 125:12, 125:13, 161:19, 163:15, 173:5, 174:19, 185:6, 187:14
concern
69:13, 184:11, 186:9, 274:7
concluded
99:15
conclusion
105:19, 271:15, 283:8, 283:9

concurrency
164:15
concurrent
142:15
condition
130:8, 140:7, 140:21
conference
29:14
confident
283:19
config
160:6, 160:7, 161:15, 161:22, 164:9, 165:3, 165:9, 165:20, 167:13, 167:14, 167:22, 169:1, 171:5, 171:19, 172:1
configuration
133:8
configure
159:21
configured
264:1
confirm
291:16
conflict
257:22
confused
54:17, 91:1, 146:9, 208:14, 208:18, 209:12, 210:9, 211:19, 229:14, 232:10, 235:20, 238:9, 267:15
confusing
144:2
connect
151:7, 151:12, 178:3, 186:14
connection
119:6, 186:21, 196:10, 196:22, 218:14, 218:17, 218:20, 219:5, 240:13, 241:22, 257:2
connections
75:16
connects
240:21
consequence
119:14, 120:2, 120:14, 120:22, 121:4
consider
9:19, 74:2, 131:20, 151:11
consistency
155:19, 157:6, 159:5, 159:11, 164:17
consistent
159:10
console
65:19, 67:5, 68:6, 68:18, 69:6, 77:8, 79:16, 83:21, 84:2, 84:4, 84:8, 84:22, 85:20, 87:14, 89:5, 94:17, 95:14, 95:15, 96:14, 97:10, 99:20, 100:1, 100:2, 100:8, 100:18, 101:2, 101:13, 101:18, 101:19, 101:21, 101:22, 102:11, 102:15, 103:5, 103:12, 105:12, 105:17, 256:1, 256:7, 256:8, 256:12, 256:16, 257:5, 257:6, 257:14, 258:8, 258:21, 274:1, 274:4
consoles
102:3, 104:16
constantly
49:22, 50:10
constitute
245:19, 246:7, 247:14
constitutes
248:6
construction
234:21
contacted
292:7
contacts
67:10, 67:14, 70:16, 71:7, 84:19, 86:1, 86:18, 87:22
content
46:17, 74:4, 179:22, 180:17, 193:5
contents
182:5, 191:21, 192:5, 193:5, 260:5
context
7:9, 7:14, 7:21, 8:6, 11:19, 32:6, 41:17, 42:5, 43:21, 55:19, 56:2, 56:12, 56:15, 60:21, 70:11, 99:5, 106:17, 106:18, 106:19, 107:10, 110:17, 113:15, 116:20, 126:13, 135:12, 135:16, 135:19, 140:20, 147:5, 152:17, 157:10, 175:22, 179:1, 196:21, 208:3, 208:17, 211:6, 218:13, 225:1, 237:4, 238:1, 238:2, 238:3, 238:18, 246:16, 247:12, 248:20, 249:4, 253:20, 255:6, 262:8, 281:6
contextual
28:13, 179:13, 179:15, 188:11, 237:6
continue
196:7, 196:8
contradict
234:22
control
45:14, 46:17, 183:10, 183:11, 183:16
convenient
102:18, 102:22, 202:22
copy
54:2, 129:14, 129:16, 135:3, 137:9, 137:10, 172:13
corp
275:22
corporate
275:20
correct
51:14, 53:21, 54:6, 95:7, 96:13, 201:15, 205:3, 229:11, 256:16, 264:22, 265:20, 294:15, 295:4
correcting
95:11, 96:6, 96:8
corrections
295:6
correctly
43:18, 205:18, 207:5, 207:7, 224:17, 224:18
correlate
38:11, 39:15, 40:3, 40:10, 41:9, 129:2
correlated
277:21

correlation
38:19, 180:6, 271:12, 277:14, 277:20, 281:22, 284:19
corresponding
213:13
cost
130:9, 131:2
could
19:21, 30:9, 47:8, 48:3, 63:5, 66:7, 67:3, 67:11, 70:5, 70:19, 79:20, 84:4, 91:20, 103:11, 104:9, 126:17, 128:10, 130:14, 133:8, 139:5, 146:10, 149:15, 178:13, 178:15, 187:21, 217:5, 223:18, 235:4, 237:21, 242:13, 246:5, 254:9, 256:15, 256:21, 257:14, 264:8, 272:2, 287:1
couldn't
70:22, 166:15
counsel
86:16, 197:8, 198:6, 198:9, 207:12, 296:11
counter
18:20, 25:15
counterpane
18:8, 19:18, 21:18, 24:13, 24:19, 24:20, 25:10, 25:19, 26:2, 26:8, 27:4, 27:21, 28:1, 28:2, 28:4, 28:11, 28:18, 28:21, 29:3, 29:7, 30:1, 30:5, 30:13, 31:9, 31:14, 32:1, 32:6, 32:14, 33:1, 33:4, 33:7, 33:13, 33:20, 35:7, 37:6, 37:15, 38:1, 45:13, 46:12, 47:13, 47:19, 48:19, 50:17, 52:4, 61:7, 267:4, 268:5, 270:22, 275:2, 275:7, 276:2, 276:17, 276:19, 278:18, 279:16, 280:3, 280:4, 280:18, 281:1, 281:3, 282:5, 282:6, 282:17, 282:20, 283:1, 283:6, 283:9, 283:22, 284:2, 284:7, 285:12, 285:20, 286:9, 286:14, 287:20, 288:4, 288:6, 288:7, 288:11, 289:1, 289:4, 289:14, 290:2, 290:5
counterpane's
17:8, 18:11, 18:12, 19:6, 19:12, 19:16, 20:1, 20:14, 22:11, 23:2, 23:11, 48:21, 48:22, 51:7, 51:11, 51:16, 267:8, 267:17, 280:6, 280:8, 280:9, 280:10, 286:6, 287:4, 289:7, 289:19
counting
282:2
couple
151:4, 164:4
coupled
9:4, 9:13, 12:22, 14:12, 35:8, 194:2, 200:21, 201:18, 226:14, 240:8
course
32:8, 45:3, 64:8, 64:10, 74:4, 92:17, 112:14, 119:5, 137:15, 156:14, 169:16, 172:20, 223:22, 243:6, 243:21, 269:5, 269:11, 270:3
court
96:11, 143:11
courtesy
96:11
coverage
39:6, 39:10
covered
27:20
covers
279:10, 285:2
cpu
42:13, 162:14, 162:17, 163:1, 165:15, 170:8, 172:18, 173:6, 173:22, 174:15, 234:5, 234:6
crashing
129:13
crazy
69:14, 182:11, 182:18, 243:1
create
66:3, 66:8, 66:20, 70:13, 72:6, 84:11, 86:4, 86:20, 137:18, 148:7, 149:22, 150:8, 220:21
creates
38:1, 158:21, 220:5
creating
225:7
credit
182:17
crime
242:10
crr
1:22, 2:11, 296:2, 297:10
currently
128:21
curse
180:11, 180:13, 181:1
customer
8:9, 8:14, 13:18, 43:13, 47:15, 47:16, 47:17, 67:13, 67:20, 68:2, 68:6, 68:15, 68:21, 69:11, 71:4, 78:15, 84:22, 85:21, 86:9, 86:15, 87:12, 87:17, 89:4, 94:10, 111:19, 240:22, 242:8, 242:22, 258:1
customer's
70:20, 71:9, 85:6, 87:4, 254:1, 258:3
customers
45:9, 46:8, 46:12, 48:8, 70:18, 71:5, 72:21, 88:18, 89:11, 89:20, 90:11, 102:4
cut
206:8
cycles
168:10

D

dad's
182:16
daniel
3:4
databases
126:11, 126:14, 126:17, 128:6, 130:14, 131:11, 131:14, 134:2, 134:6, 134:12, 149:14, 151:4, 151:6, 152:7, 156:14
date
295:10
day
38:7, 147:8, 170:7, 297:3
dc
3:7
deal
72:18
debt
150:1
decide
40:5, 119:6, 187:1, 188:12, 209:6, 281:10
decided
219:1
decides
195:21
decision
195:18, 211:5, 214:22, 215:1, 215:9, 216:3, 219:15, 291:19
decisions
218:2
declaration
5:13, 5:19, 6:1, 11:1, 11:21, 19:21, 24:7, 27:3, 28:7, 30:6, 31:8, 54:3, 92:10, 92:21, 174:22, 178:22, 193:8, 204:18, 204:21, 205:5, 205:7, 210:6, 215:12, 220:1, 224:10, 229:10, 235:6, 245:8, 254:14, 259:7, 261:17, 262:1, 262:3, 262:10, 263:7, 263:17, 266:14, 267:7, 271:2, 271:20, 276:10, 290:13, 290:19
decorum
21:3
deep
51:21
default
135:3
defer
294:10
deferred
193:14, 195:22, 196:2, 218:3, 218:4, 219:2, 219:3, 224:13, 224:20, 225:11, 225:21, 226:3, 226:6, 229:12, 230:10, 230:16, 293:20, 294:4
define
147:5, 173:21
defined
111:13, 133:15, 199:5
definitely
49:18
definition
64:7, 97:19, 109:9, 120:11, 120:12, 121:5, 138:4, 231:19, 233:2
delete
6:4, 6:9, 141:17, 143:7
demand
141:19
denial
46:17
department
191:3
depend
169:2
dependency
146:15, 146:18
depending
102:3, 107:18, 110:7, 128:19, 142:3, 164:7, 213:20, 246:19, 257:21
depends
73:18, 75:1, 107:12, 111:17, 113:10, 113:15, 126:22, 130:19, 132:7, 134:20, 138:8, 146:14, 146:15, 147:4, 151:9, 165:8, 166:2, 166:8, 172:9, 174:15, 189:20, 237:4, 237:22, 238:15, 272:13
depicted
217:11, 217:17, 218:8
deploy
50:9, 59:9
deponent
295:1
deposition
1:13, 2:1, 64:12, 91:16, 296:6, 296:7, 296:8, 296:12, 296:13
derived
16:1
describe
108:4, 108:18, 109:15, 115:2, 146:9, 160:11, 229:19
described
61:10, 61:11, 65:3, 79:21, 82:17, 85:4, 166:10, 167:2, 210:21, 221:17, 228:22, 242:15, 252:22, 258:16, 262:20, 283:6, 283:19
describes
56:5, 255:8
describing
213:3, 227:8, 228:6, 253:13
description
40:22, 41:6, 41:10, 43:20, 47:2, 48:20, 57:16, 59:4, 63:13, 75:3, 102:14, 109:9, 121:22, 123:16, 131:22, 133:11, 157:12, 231:5, 241:17, 241:19, 242:13, 242:16, 244:2, 248:12, 250:3, 256:19, 291:1
design
58:13
detail
39:4, 39:13, 136:3, 213:20, 214:5, 221:17, 247:18, 248:18, 253:5, 255:15
detailed
241:17, 241:19, 242:4, 242:13, 242:16, 244:1, 248:11, 250:3, 256:19
details
11:20, 22:19,

52:21, 57:15, 80:3, 131:6, 132:16, 132:19, 132:20, 132:21, 135:9, 159:14, 167:19, 168:6, 171:10, 174:14, 174:19, 211:12, 241:17, 242:14, 242:15, 246:20, 248:14, 250:11, 254:7, 254:11, 256:11
detect
69:16, 77:9, 135:12, 135:13, 232:18, 234:9, 278:19
detected
58:11, 60:7, 61:19, 62:15, 63:11, 65:4, 73:6, 77:4, 79:6, 80:9, 80:10, 80:18, 81:8, 82:17, 83:15, 273:7, 277:19
detection
39:11, 40:13, 40:17, 43:3, 43:8, 44:21, 50:12, 52:16, 55:12, 58:15, 64:4, 194:19, 195:2, 195:4, 220:16, 221:5, 222:13, 222:16, 222:17, 223:18, 223:20, 224:6, 231:17, 231:19, 231:20, 232:4, 232:9, 232:12, 232:15, 232:18, 233:2, 233:8, 233:21, 234:13, 275:6, 276:18, 277:2, 277:6, 278:6, 278:8, 278:9, 278:14, 278:17, 278:21, 279:2, 279:11, 279:17, 279:20, 280:2, 280:7, 280:8, 280:22, 281:3, 281:12, 281:21, 282:4, 282:7, 282:16, 282:19, 282:21, 283:10, 283:22, 284:11, 285:2
detection's
220:19
detects
292:8, 293:9
determine
105:7, 293:14
determined
293:19, 293:20
development
283:17
device
269:16
devices
34:12, 35:3, 36:20, 38:8, 38:12, 38:20, 268:11
devil
132:19, 132:21
different
7:9, 7:10, 11:22, 23:16, 59:15, 60:14, 60:16, 60:17, 62:12, 62:13, 62:22, 63:16, 63:21, 90:3, 94:9, 94:13, 101:21, 103:12, 107:1, 110:14, 127:11, 133:1, 135:2, 135:6, 145:2, 147:9, 149:9, 153:15, 154:7, 154:12, 156:13, 156:17, 158:15, 159:1, 160:11, 163:15, 163:20, 164:9, 164:15, 168:20, 181:8, 192:10, 193:6, 209:11, 217:14, 221:8, 221:19, 222:5, 222:21, 243:10, 253:10, 253:15, 256:20, 258:14, 273:12, 281:13, 282:4, 286:5
difficult
162:5
direct
82:16, 193:14, 225:22
direct-action
225:19, 228:1, 228:7, 229:18
directed
6:21, 17:20, 18:2
direction
196:4
directly
80:6
disagree
203:9, 230:8, 252:13
discard
110:2, 113:20, 118:16, 118:20, 119:4, 188:17
discarded
35:14, 107:8, 115:6, 115:17, 117:14, 119:20, 120:9, 120:19, 194:8, 199:18, 199:22, 200:1, 202:2, 202:10
discarding
114:19, 119:10, 121:13, 189:2, 230:21, 230:22, 231:1
discards
108:13
discern
76:10
disclosed
116:4, 223:2, 229:17, 229:21, 255:2
discloses
226:13, 226:19, 227:17, 229:22, 261:18, 263:8, 263:17
disclosing
227:5
disclosure
239:17, 257:12
disclosures
248:22
discover
55:17, 254:22
discoveries
70:15, 71:20, 84:18, 87:21
discovery
67:9
discrete
275:5, 277:17, 277:18
discrete-filtering
281:7
discuss
24:3, 27:15, 56:10
discussed
253:2, 288:1
discusses
158:19
discussing
52:11, 247:11
discussion
123:16, 182:16, 286:13, 288:22
disinteresting
121:13
displayed
46:8, 256:9

dispute
291:5
disputing
207:19, 290:22, 291:6
distinct
220:6
distinguished
280:11, 281:3, 282:8
distinguishes
276:17
distinguishing
280:13
distributed
151:19, 152:2, 158:17
distributor
155:17
document
5:11, 24:11, 25:7, 38:3, 46:2, 52:19, 55:9, 66:13, 81:1, 87:11, 87:20, 88:6, 88:13, 89:7, 90:17, 90:20, 91:3, 93:6, 93:13, 98:22, 128:12, 128:14, 129:21, 130:8, 131:7, 132:22, 179:2, 225:2, 235:3, 236:4, 239:10, 263:13, 268:1, 271:13, 285:4
documentation
29:22, 30:4
documents
29:2, 46:1, 46:2, 82:12, 87:10, 87:16, 88:22, 90:3, 90:7, 91:19, 92:3, 92:11, 92:17, 95:1, 126:1, 131:22, 132:20, 133:11, 178:2, 285:5
doing
12:7, 13:18, 13:19, 28:15, 31:17, 38:17, 39:5, 43:12, 67:5, 85:11, 86:17, 89:2, 89:6, 91:21, 91:22, 92:1, 92:2, 92:6, 93:11, 93:12, 94:7, 94:13, 94:14, 94:21, 94:22, 118:11, 118:12, 124:9, 131:2, 131:6, 136:9, 136:10, 141:2, 154:21, 155:6, 157:4, 159:7, 163:1, 163:4, 163:5, 163:9, 168:10, 170:9, 173:13, 173:14, 174:17, 184:3, 184:4, 184:18, 187:7, 188:7, 189:5, 196:19, 209:11, 214:1, 214:13, 216:9, 220:19, 222:7, 225:12, 225:14, 229:12, 230:3, 230:11, 230:20, 230:21, 231:1, 231:2, 247:18, 248:15, 253:13, 254:8, 254:10, 256:20, 258:14, 269:4, 270:5, 281:6, 284:10, 284:11, 286:20
domain
126:9
dominated
275:21
done
15:9, 24:22, 25:3, 44:11, 99:17, 140:2, 144:18, 148:15, 197:9, 198:6, 202:17, 216:12, 223:7, 278:5, 281:11, 294:18
double-check
30:11
down
34:21, 47:15, 49:19, 50:2, 50:4, 50:13, 50:18, 74:9, 142:18, 143:1, 144:7, 145:11, 147:12, 148:6, 152:19, 153:22, 155:9, 164:22, 241:3, 292:17, 293:17
download
48:12, 183:20, 186:6, 187:20, 192:20
downloading
177:18, 181:19, 185:11, 186:1, 186:10, 187:17
dr
5:8, 51:6, 51:7, 106:3, 151:1, 212:2, 212:4, 259:6, 291:13, 291:15
draw
105:19, 271:14, 283:7
drive
127:2, 127:3, 129:7, 131:5
driver
182:6
due
21:8, 95:22, 96:5, 272:3, 285:20, 287:4, 288:17, 289:14
duh
186:14
duly
5:3, 296:6
duration
164:6
during
45:16, 158:4, 158:6, 163:18, 166:11, 172:15, 172:16, 173:2, 173:9, 173:18, 174:11, 191:3
duvall
175:4, 175:20, 175:21, 185:8, 190:16, 191:10, 191:12, 191:15, 191:19, 192:4, 192:11, 192:16, 192:22, 195:13, 195:16, 196:19, 197:1, 198:3, 216:22, 217:5, 225:17, 226:4, 226:13, 226:19, 227:4, 227:9, 227:17, 227:22, 229:3, 229:20, 229:22, 230:17, 245:15, 246:3, 246:17, 248:22, 249:6, 249:8, 249:10, 249:14, 250:20, 251:8, 252:1, 252:4, 252:9, 252:13, 291:15, 291:18
duvall's
181:4, 181:5, 191:15, 192:8, 193:14, 228:6, 229:16, 229:17
duvall-chu
260:21, 261:3, 264:10

duvall-chu's
259:17
dynamic
47:9, 48:9, 49:16, 130:22, 132:15, 133:17, 134:3, 134:5, 134:10, 135:11, 140:8, 140:9, 140:19, 147:15, 148:1, 148:2, 154:9, 154:10, 165:3
dynamically
45:15, 47:4, 48:4, 48:22, 126:18, 126:21, 135:17, 137:2, 155:11, 155:12, 156:1, 156:20, 157:15, 158:4, 158:8, 159:14, 159:15, 162:9, 163:16, 163:19, 163:22, 166:11, 169:8, 170:3, 170:16, 170:20, 171:10, 289:15

E

each
17:6, 63:22, 73:11, 94:8, 134:21, 233:6
earlier
32:13, 112:4, 125:21, 207:19, 247:2, 247:10, 253:1, 253:2, 271:4, 280:17
early
48:15, 49:17, 56:21
easier
159:5
easiest
234:12
education
290:18
educational
187:10
edward
3:12
effect
213:16
efficiency
149:2
either
47:9, 78:18, 126:18, 159:13, 162:15, 163:13, 191:13
electronic
275:21
electronics
256:13
element
12:16, 14:5, 15:15, 25:11, 27:4, 31:10, 33:13, 33:21, 36:10, 37:8, 45:13, 106:8, 176:12, 199:8, 200:18, 221:2, 221:10, 221:21, 227:9, 228:8, 229:19, 229:20, 239:1, 239:2, 240:4, 243:12, 267:11, 267:21, 269:19, 271:1
elements
17:7, 26:5, 26:6, 26:7, 26:9, 228:14, 237:6, 237:13, 278:22, 290:8
eleven
2:6, 3:14, 296:15
else
117:19, 126:9, 143:6, 143:15, 149:1, 150:7, 150:10, 156:6, 156:8, 168:16, 173:15, 180:1, 203:16, 222:14, 223:18, 224:5, 236:2
email
59:16, 178:1, 178:12, 180:2
embodies
20:22
embodiment
19:7, 19:13, 19:19, 20:2, 20:5, 20:10, 20:15, 21:5, 21:7, 21:17, 21:22, 22:22, 23:9, 23:21, 26:15, 30:19, 31:14, 31:22, 36:18, 158:2, 221:6, 231:11, 268:5, 280:19, 284:7, 286:18, 288:7, 289:1, 290:2
embodiments
242:4
embody
19:16
emergence
58:5, 79:19
emergency
247:19
emerges
58:1
emphasize
255:11
emphasized
32:7, 43:6
emphasizing
84:21, 86:2, 258:17
empirically
16:1
employed
296:20
enable
193:2, 216:16
enables
280:22
encompassed
232:11
encrypt
243:4, 243:7, 243:21
encrypted
38:13, 38:14, 243:14
end
28:9, 83:12, 94:10
enforce
190:7, 215:1, 215:9
engage
198:20
engine
37:2, 37:11, 42:2, 74:11, 80:13, 101:5, 105:4, 105:12, 115:10, 221:1, 221:9, 222:3, 223:2, 223:7, 270:12
engine's
99:22
engines
65:18, 67:16, 68:11, 72:14, 75:7, 79:15, 100:19, 102:2, 103:6, 103:16, 104:6, 256:6, 273:22, 274:3
english
207:14
enough
31:22, 40:20, 61:1, 74:12, 92:8, 163:8, 166:21, 186:22, 238:6, 247:17, 248:14, 248:18, 250:11, 253:5, 255:15

ensemble
245:3, 248:1, 277:12
ensure
142:12
entail
106:15, 106:20, 231:15
entails
108:5
enter
182:17
entered
275:2
entirely
255:8, 255:9, 255:11
entirety
56:5
entrances
276:2
epoch
162:19, 163:18, 164:1, 164:6, 164:8, 164:9, 165:12, 165:13, 165:14, 165:19, 165:21, 166:12, 166:16, 166:17, 169:12, 169:13, 170:8, 170:9, 170:12, 170:17, 170:18, 172:15, 172:17, 172:19, 173:2, 173:7, 173:9, 173:13, 173:15, 173:16, 173:18, 173:20, 174:10, 174:11
epochs
164:4, 165:2, 166:4
equate
173:5
equivalence
145:10
equivalent
142:4, 143:17, 145:10, 145:13, 152:17, 154:5, 155:6, 156:7
equivalents
156:12
errata
295:7
escamilla
52:17
esquire
3:3, 3:4, 3:11, 3:12
essential
67:3, 149:3, 278:22
essentially
24:19, 31:3, 40:1, 56:1, 105:2, 143:14, 144:4, 145:8, 147:12, 148:6, 153:22, 154:7, 164:22, 167:8, 168:1, 173:3, 179:13, 195:8, 195:16, 196:3, 198:19, 199:21, 216:1, 216:3, 225:5, 229:2, 229:16, 240:20, 241:10, 241:12, 248:13, 253:7, 265:4, 279:10, 280:1, 280:21, 286:8, 286:15, 289:8, 290:6, 293:9
establishing
241:11
even
29:11, 44:5, 51:16, 55:14, 129:14, 129:15, 147:13, 151:12, 151:13, 163:8, 164:19, 176:21, 177:6, 180:1, 185:6, 186:20, 187:5, 197:22, 232:12, 233:19, 243:3, 248:16, 266:2, 277:20
event
14:7, 14:20, 46:7, 58:10, 58:12, 61:19, 62:15, 62:16, 63:11, 65:4, 65:6, 65:7, 73:20, 73:22, 74:13, 76:15, 78:17, 79:5, 79:7, 79:22, 80:1, 80:8, 80:9, 80:11, 80:12, 80:15, 80:16, 81:4, 81:5, 81:8, 81:10, 81:12, 81:13, 81:20, 81:21, 82:1, 82:17, 83:15, 83:20, 84:14, 97:13, 99:15, 103:13, 103:20, 103:21, 104:5, 104:19, 105:2, 105:5, 105:7, 105:13, 105:17, 177:19, 178:9, 178:13, 178:15, 178:18, 194:19, 222:13, 236:17, 273:7, 273:9, 273:11, 273:12, 274:3, 274:11, 277:18, 277:19, 277:22
event's
60:7
events
9:14, 12:11, 13:1, 13:6, 13:12, 14:1, 14:13, 14:20, 14:22, 15:13, 35:10, 68:8, 69:16, 73:6, 75:21, 76:21, 77:3, 97:18, 97:21, 98:3, 99:17, 107:4, 109:7, 176:14, 176:17, 176:19, 176:20, 176:21, 176:22, 177:1, 177:2, 177:3, 177:4, 177:5, 177:7, 177:8, 177:10, 177:13, 188:17, 188:18, 194:3, 199:15, 201:7, 214:17, 240:6, 240:9, 254:2, 272:17, 274:4, 274:20, 284:16
ever
11:5, 11:18, 12:2, 79:1, 133:20
every
20:15, 22:6, 22:10, 22:12, 23:3, 32:11, 55:12, 96:8, 140:11, 163:2, 163:10, 169:12, 173:7, 205:5
everybody
82:6, 133:15, 143:15, 258:8
everything
82:5, 116:8, 146:16, 156:6, 156:8, 163:8, 166:21, 168:16, 177:15, 177:22, 178:5, 180:1, 186:18, 188:1, 188:2, 204:22
evidence
87:10, 87:19, 92:16, 93:6,

180:5, 180:15, 180:22, 184:20, 185:3, 185:4, 186:19, 197:2, 245:19, 246:7, 247:15, 248:6, 249:21, 270:21, 282:17
ex-force's
70:16
exact
56:22, 75:5, 155:21, 170:9, 246:19
exactly
18:15, 32:15, 40:16, 43:2, 43:4, 43:11, 48:7, 57:16, 63:13, 72:10, 74:21, 80:11, 80:19, 82:12, 89:2, 93:10, 93:11, 94:18, 111:17, 112:13, 113:9, 113:14, 114:14, 118:10, 121:7, 122:3, 130:19, 131:1, 154:2, 170:4, 179:8, 187:3, 187:6, 189:5, 189:18, 190:8, 190:9, 190:10, 195:6, 216:5, 228:20, 287:21, 289:21
examination
4:6, 5:6
examine
31:22
examined
5:4, 295:3
example
8:5, 8:20, 18:21, 42:16, 42:19, 46:9, 46:22, 47:2, 69:17, 82:9, 107:21, 107:22, 110:13, 125:7, 132:2, 133:6, 148:9, 149:12, 153:8, 155:16, 156:4, 158:15, 168:6, 171:12, 180:9, 180:10, 191:2, 192:17, 192:18, 212:15, 212:16, 212:18, 213:5, 215:1, 221:6, 228:15, 228:17, 229:5, 234:5, 234:13, 236:22, 237:2, 237:16, 237:20, 239:18, 242:4, 244:12, 244:13, 244:19, 246:17, 247:6, 247:14, 247:21, 248:20, 249:4, 256:9, 256:14, 267:21, 268:8, 271:12, 284:19, 286:6
examples
8:5, 15:3, 15:13, 53:15, 108:21, 109:1, 110:12, 171:15, 234:2, 248:2, 255:2, 255:21
except
142:19, 143:15, 152:14, 213:3
exclude
20:18, 21:12
exhibit
5:10, 6:12, 37:21, 41:11, 46:1, 46:5, 47:3, 52:16, 54:2, 56:10, 57:6, 57:9, 65:10, 216:22, 247:2, 247:5, 247:14, 248:3, 248:6, 248:20, 249:4, 249:20, 252:22, 253:12, 255:2, 255:21, 256:2, 257:12, 271:1, 273:5, 273:20, 275:12, 282:13, 283:12, 288:2
exhibits
4:11
experience
47:11, 88:10, 136:4, 186:20, 257:19, 290:18
experienced
134:11
expert
36:8, 58:10, 61:20, 62:15, 62:17, 63:12, 65:4, 65:6, 79:1, 79:6, 79:8, 79:17, 80:5, 80:8, 80:10, 80:11, 80:19, 80:20, 81:3, 81:9, 81:11, 82:2, 82:15, 82:20, 83:16, 85:10, 87:2, 88:9, 88:16, 89:17, 95:9, 95:10, 95:19, 180:5, 229:9, 230:6, 251:6, 251:21, 252:10, 256:14, 257:13, 263:2, 273:11, 290:19
expert's
52:12, 262:1, 262:9, 266:5, 266:6
expertise
8:19, 92:12, 92:22
experts
58:7, 58:11, 60:11, 63:3, 64:17, 64:19, 66:2, 70:12, 72:5, 73:1, 78:18, 79:5, 79:20, 84:3, 84:11, 93:19, 93:20, 175:3, 245:12, 253:8, 273:8, 291:1
expires
297:5
explain
27:1, 161:1, 207:10, 213:1, 218:4, 288:5
explained
197:21, 264:3, 265:3, 287:22
explains
217:14, 226:6, 239:18
explanation
242:5, 243:19, 251:9
explicitly
16:10, 17:1, 18:6, 19:4, 30:17, 31:7, 48:12, 243:3, 274:15
express
92:10, 92:21, 261:16
expressed
10:22, 11:12
extent
129:19, 290:8
extracted
236:13

F

f-o-r-m
115:19
face
138:11

facebook
191:2
fact
43:1, 48:9, 51:16, 128:8, 154:12, 156:16, 162:2, 169:5, 174:14, 182:2, 182:6, 182:11, 182:15, 277:21
factors
131:20
facts
237:9
fair
47:9, 61:14, 73:15, 78:19, 97:14, 98:8, 104:7, 154:5, 212:22, 225:19, 226:5
fairness
149:3, 149:4
fall
18:21
falls
22:11
familiar
45:21, 127:22, 134:14, 134:18, 136:5, 217:3
fan
186:5
far
94:10, 249:12
fast
165:9
feature
33:12, 33:19, 205:12, 214:1, 229:19
features
33:17, 45:21, 151:5, 276:16, 279:16, 280:13, 288:13, 288:17, 290:4
february
5:20
fee-based
58:5
feedback
15:16, 15:22, 16:3, 16:6, 16:12, 16:16, 16:17, 16:20, 17:15, 45:17, 46:10, 279:12, 281:17, 284:22
feel
48:13, 163:6, 163:8, 166:21
fetching
249:13
few
102:20, 175:16
field
92:13, 144:11, 232:6, 234:4
fields
236:13, 236:20
figure
8:4, 8:18, 13:15, 13:17, 39:18, 39:21, 39:22, 41:1, 41:2, 43:12, 43:16, 56:8, 75:6, 86:9, 87:4, 88:18, 109:20, 110:17, 118:8, 162:7, 176:11, 179:9, 194:11, 194:12, 195:14, 195:15, 196:15, 196:19, 200:14, 200:16, 217:5, 217:7, 217:12, 217:15, 217:17, 217:18, 217:21, 218:4, 218:10, 218:15, 218:16, 218:19, 219:3, 219:6, 219:10, 220:11, 221:5, 221:18, 222:12, 225:18, 225:20, 226:2, 229:3, 229:17, 229:18, 229:20, 229:21, 231:10, 241:6, 242:5, 253:21, 279:8, 291:18, 292:1, 292:4, 292:18, 293:7, 294:13
figures
194:21, 199:6, 217:10, 243:19
figuring
162:8
file
138:4, 138:5, 138:9, 138:10, 144:4, 144:5, 144:7, 159:21, 160:6, 160:7, 161:15, 161:22, 164:9, 165:3, 165:9, 165:20, 167:13, 167:14, 167:22, 168:14, 169:1, 171:5, 171:19, 172:6
files
172:1
filter
13:20, 34:13, 35:3, 36:21, 41:12, 41:13, 45:6, 107:14, 110:1, 120:15, 189:18, 190:8, 203:5, 203:6, 203:22, 204:1, 204:12, 205:15, 205:16, 205:22, 206:1, 207:21, 207:22, 208:20, 208:21, 210:8, 210:17, 210:18, 212:21, 215:15, 215:22, 216:6, 224:20, 232:22, 268:12, 269:17, 285:21, 285:22, 287:5, 287:6, 292:5, 293:22
filtered
108:12, 117:22, 194:16, 199:10, 204:11, 212:6, 232:21, 267:10, 267:19, 267:20, 286:1, 287:7
filters
34:13, 35:3, 36:21, 38:9, 38:10, 41:7, 41:21, 41:22, 43:20, 111:17, 158:1, 172:5, 195:9, 206:4, 224:13, 225:19, 226:3, 228:1, 228:7, 229:18, 267:8, 267:9, 267:18, 268:12, 269:17, 270:5, 271:7
financially
296:22
find
66:3, 66:8, 70:12, 70:19, 72:5, 72:11, 84:11, 84:12, 86:4, 88:19, 93:20, 102:18, 108:22, 116:6, 171:14, 181:3, 190:5, 233:9, 233:10, 233:11
finding
72:7, 86:20
fine
48:7, 64:13, 97:4, 168:9, 202:18, 236:1
finish
77:17, 143:16, 148:22, 154:22, 155:1, 255:17

finished
155:9, 279:4
firewall
75:15, 211:8,
213:5, 213:7,
213:12, 215:2
firewalls
46:13, 191:1,
214:20, 214:21
first
9:7, 9:19,
10:1, 10:5,
10:7, 10:12,
10:18, 11:2,
11:6, 11:14,
12:4, 25:15,
26:20, 43:15,
51:17, 52:1,
72:4, 78:22,
79:12, 86:19,
104:20, 108:12,
114:2, 139:20,
144:19, 145:17,
146:3, 146:11,
146:12, 147:1,
148:8, 148:12,
148:13, 149:15,
149:16, 152:5,
160:22, 170:17,
181:22, 182:3,
182:14, 186:4,
189:15, 191:19,
195:18, 196:4,
196:9, 196:12,
196:21, 197:16,
198:14, 198:17,
205:11, 205:20,
217:18, 218:15,
219:6, 219:12,
219:15, 224:6,
227:15, 228:16,
232:9, 234:10,
240:18, 245:11,
245:13, 246:5,
252:5, 259:9,
259:15, 265:3,
268:16, 271:22
fits
39:20
five
91:7
flight
53:10
flip
129:12, 196:1
flow
75:18, 194:21,
195:17
flowchart
217:16
fly
138:10
focus
44:7, 214:17,
223:13, 224:3,
268:19
focusing
214:17
follow
151:4
followed
9:16, 35:12,
107:6, 194:5,
199:16, 201:9,
221:13, 223:8,
261:4, 264:11
following
189:14
follows
5:5, 53:8,
220:7
food's
150:19
foregoing
295:3
foreign
183:1, 185:6
forever
50:8, 168:22,
233:12
forgot
263:14
format
74:3, 74:21,
274:16
formed
188:5
former
47:12, 48:18
forming
116:16, 225:7
forms
116:12
formulated
29:10
forth
113:12, 130:9,
133:18, 177:12,
254:6, 257:3,
271:18, 277:15,
282:2, 284:20,
296:6
fortinet
235:11, 235:12,
254:15
forward
196:6
forwards
108:16
found
70:6
founded
29:7
four
90:15, 164:13
fourth
57:22, 79:2
fox
3:5
frame
49:6, 49:15,
92:5
free
207:16
frequencies
282:2
frequency
74:22, 277:15
friends
157:4
front
5:10, 6:11,
35:20, 58:12,
84:4, 87:10,
91:19, 96:2,
226:9, 257:14
fully
196:14
function
209:10, 213:13,
215:4, 216:13,
216:19, 281:7
functionality
33:4, 33:6
functions
90:3, 275:5,
279:1
fundamentally
167:1
further
27:1, 37:2,
37:12, 40:10,
42:3, 43:3,
43:14, 44:13,
115:10, 217:14,
218:3, 234:12,
241:3, 241:7,
244:21, 258:20,
265:6, 268:8,
270:13, 271:10,
281:19, 281:20,
284:18, 293:17,
296:10, 296:13,
296:18
furthers
263:20

G

gateway
240:19, 240:20,
241:5
gather
188:8
gave
15:3, 15:12,
32:5, 56:12,
73:5, 121:4,
196:21
gee
49:20, 50:18
general
7:15, 7:20,
7:22, 8:1,

33:11, 74:16, 93:7, 93:8, 93:15, 96:21, 98:12, 98:13, 98:16, 98:20, 99:2, 107:11, 113:5, 113:8, 113:12, 113:14, 113:17, 113:19, 114:1, 114:22, 147:22, 149:21, 154:19, 165:10, 274:17
generally
113:16, 113:21
generate
115:3, 115:4
generic
98:11
gist
184:2
give
17:4, 24:12, 25:5, 30:9, 41:20, 44:11, 48:10, 80:22, 82:11, 87:15, 89:6, 96:11, 107:19, 107:20, 109:5, 114:15, 131:7, 132:2, 157:12, 159:14, 163:1, 174:16, 192:18, 216:3, 231:10, 234:2, 255:14, 256:11, 275:11, 285:4, 287:13, 287:16
given
7:9, 11:18, 220:22, 295:5, 296:9
gives
242:4
giving
29:14, 197:1, 279:12, 284:22
gloss
99:19
go
5:16, 15:2, 15:4, 22:19, 31:16, 32:11, 37:21, 39:13, 39:22, 48:11, 62:17, 65:22, 75:19, 77:20, 81:17, 93:2, 108:6, 108:17, 116:9, 119:6, 119:7, 129:12, 139:14, 140:3, 162:20, 169:16, 169:20, 170:1, 172:13, 174:21, 178:2, 178:5, 180:18, 180:20, 183:19, 184:7, 184:9, 184:19, 185:2, 185:21, 196:6, 196:7, 200:9, 200:10, 208:7, 209:7, 218:18, 219:18, 219:20, 220:12, 228:20, 233:12, 239:1, 245:6, 250:14, 263:11, 266:12, 271:19, 274:21, 290:3, 291:15, 291:20, 292:14, 293:13, 294:3, 294:4, 294:10, 294:11
goal
107:13
goes
39:4, 43:7, 116:12, 195:19, 220:13, 227:22, 240:1
going
12:10, 15:7, 41:3, 49:20, 50:19, 53:19, 63:18, 67:15, 72:15, 78:8, 79:9, 80:21, 82:21, 85:1, 85:2, 87:18, 89:8, 91:18, 92:8, 96:10, 102:17, 111:1, 113:11, 129:9, 129:11, 129:18, 131:19, 132:17, 133:18, 135:18, 138:18, 142:20, 145:20, 149:5, 150:7, 150:8, 150:14, 159:7, 181:6, 182:19, 187:22, 189:22, 190:1, 202:21, 212:20, 223:20, 225:17, 242:6, 261:11, 278:20, 289:5
goldstein
3:5
gone
156:3
good
5:8, 42:21, 42:22, 44:17, 44:22, 150:16, 203:6, 204:1, 205:16, 206:2, 208:6, 210:18, 213:8, 232:21
google
234:1
ground
140:12, 142:7
guarantee
142:6
guaranteed
142:13
guess
9:18, 37:19, 89:16, 106:14, 117:3, 135:21, 136:2, 152:22, 208:13, 212:5, 222:5, 222:20, 231:13, 232:10, 243:9, 243:10, 285:15
guilty
184:21
guy
180:16
guys
71:10

H

hackers
58:14
hand
52:15, 54:1, 74:7, 186:12, 258:15, 287:15, 297:3
handed
37:20, 54:2
handing
216:21
handle
94:19, 113:11
handles
195:20
handling
127:17, 196:20
hands
60:13
happen
49:21, 67:8, 139:12, 149:18, 225:10
happening
65:8, 76:21, 166:19
happens
98:18, 173:18
happily
147:21
hard
127:2, 127:3, 129:5, 129:10, 129:19, 131:5, 131:20, 133:14, 137:11, 140:8, 140:22, 148:2,

148:4, 168:15, 185:7, 223:19
header
285:10
heading
53:1, 57:20, 58:1, 65:11, 175:3, 193:10, 193:11, 266:3, 285:10
hear
96:1
heard
18:8, 73:7, 91:5, 95:6, 95:8, 96:4, 127:5, 127:19, 127:21, 127:22, 133:20, 134:11
held
2:1
help
15:7, 52:14, 55:17, 58:12, 62:16, 63:12, 65:5, 74:5, 79:7, 79:21, 80:16, 81:3, 83:16, 143:11, 187:6, 254:22, 260:11, 264:8, 273:8, 275:11
here
22:9, 23:14, 37:18, 38:3, 38:4, 43:5, 48:8, 55:15, 57:4, 59:4, 60:6, 60:20, 61:3, 61:10, 62:14, 68:6, 71:3, 77:5, 80:6, 82:17, 87:2, 87:21, 88:16, 89:15, 89:18, 94:10, 94:21, 99:5, 99:8, 100:16, 102:14, 105:11, 108:8, 108:17, 109:9, 110:11, 110:19, 110:20, 120:8, 129:22, 130:12, 131:9, 133:10, 135:16, 136:15, 147:19, 149:13, 150:19, 158:22, 162:5, 167:3, 167:12, 168:6, 168:20, 179:2, 179:17, 181:17, 190:21, 192:2, 195:4, 197:3, 204:10, 205:21, 211:8, 213:15, 216:15, 220:10, 225:1, 225:3, 225:11, 225:16, 226:22, 235:1, 240:16, 241:4, 252:8, 263:12, 265:11, 266:5, 271:11, 277:9, 286:7, 287:19, 293:1, 293:8
here's
82:13, 94:21
hereby
295:2, 296:4
hereinbefore
296:6
hereunto
297:2
hey
22:18, 23:17, 24:2, 29:20, 40:18, 45:1, 59:6, 59:8, 59:14, 60:13, 61:2, 65:7, 81:20, 82:7, 87:16, 90:21, 114:12, 122:17, 131:6, 135:12, 150:6, 160:6, 168:7, 172:10, 174:14, 183:13, 187:22, 188:7, 192:2, 205:21, 206:5, 210:20, 215:1, 258:7, 270:4, 277:20, 287:16, 289:3
hierarchical
144:4, 168:14
high
38:16, 179:6
highlight
67:11
history
283:18
hit
150:15, 202:22
hold
32:15, 54:15, 83:7, 98:19, 116:20, 154:21, 265:1
holder
3:10
honest
122:15
hopefully
17:13
host
292:6
hosted
185:1
hosting
180:18, 183:18
hour
102:18, 103:1, 150:15, 202:22
hours
191:4
human
15:16, 16:4, 16:6, 16:10, 16:13, 16:17, 16:20, 17:2, 17:16, 59:20, 60:3, 61:13, 61:21, 66:7, 70:6, 272:1, 272:2, 272:7, 272:10, 272:22, 273:10, 273:16
humans
272:18
hundred
139:19, 168:8
hung
123:2
hypothetical
85:3, 152:11, 153:7, 154:17, 165:7, 166:1, 166:7, 167:16

I

ibm
52:3, 52:7, 57:8, 57:11, 57:19, 58:21, 60:3, 61:3, 61:9, 61:12, 62:14, 63:11, 64:20, 65:4, 70:2, 70:3, 76:5, 77:3, 77:4, 77:14, 78:14, 79:3, 79:6, 79:19, 80:10, 80:12, 80:22, 81:3, 81:11, 82:11, 88:22, 89:9, 90:10, 93:4, 95:4, 247:6, 247:19, 252:7, 255:1, 255:20, 258:12, 272:22, 273:7, 275:21, 276:8, 276:11, 282:15, 282:18
ibm's
53:8, 58:1, 58:4, 58:7, 58:11, 60:12, 63:4, 63:5, 64:17, 78:18,

80:14, 86:8, 87:3, 88:17, 89:19, 282:9
idea 133:15
ideas 43:7
identification 104:4, 176:16, 236:15, 236:16
identified 13:1, 13:12, 13:22, 14:13, 14:21, 14:22, 15:13, 75:21, 76:15, 97:18, 99:17, 109:7, 177:13, 239:22, 240:6, 240:9, 274:19, 284:16
identify 9:14, 14:20, 35:9, 66:19, 74:12, 89:11, 89:20, 90:12, 107:3, 110:3, 110:18, 111:13, 117:21, 118:16, 133:5, 176:13, 177:12, 188:16, 189:8, 194:3, 199:14, 201:6, 203:13
identifying 259:18, 264:5, 265:4, 265:10, 265:13, 265:14, 266:8, 266:11, 279:9, 281:20
ids 65:15, 275:4
ignore 119:5
ill 188:5
illustrated 229:5
imagine 145:14, 146:17, 151:16, 153:11, 169:10, 213:2, 223:19
imagining 152:1
immediate 218:3, 293:15, 293:19, 294:9
immediately 242:19
impact 167:2, 167:12
implement 81:19, 81:20, 82:10, 108:19, 111:9, 111:16, 114:12, 114:13, 114:14, 115:22, 117:10, 121:7, 121:11, 159:19, 161:13, 171:4, 171:18, 182:3, 189:16, 190:1, 190:6, 190:11, 190:22, 191:4, 222:22, 233:8, 244:5
implementation 96:20, 148:20, 167:18, 171:10, 211:12, 213:19, 214:5
implemented 174:16, 213:17, 215:7, 290:5
implementing 111:18, 190:16, 244:1
implications 179:8
important 60:9, 70:15, 80:4, 82:15, 100:5, 195:22, 251:16
impression 163:1
improve 126:4, 249:17
inaccessible 152:7, 153:4, 154:15
inc 1:5, 1:9, 296:11
incidents 239:22
include 20:19, 48:4, 57:8, 97:12, 176:19, 177:2, 177:4, 236:12, 242:15, 244:4, 252:16, 264:4, 265:5, 265:7, 284:19
included 22:2, 22:3, 232:14
includes 9:16, 35:8, 35:11, 107:6, 194:5, 199:16, 201:1, 201:2, 201:8, 226:15, 227:19, 244:14, 245:1, 263:22, 267:8, 267:18, 281:22
including 12:3, 38:7, 38:8, 38:20, 103:12, 107:5, 178:1, 178:2, 211:2, 245:13, 274:6, 274:7
inconsistency 140:14, 148:7
incorporate 181:4, 181:6
indeed 275:1
indicate 228:1
industry 29:6, 128:8, 131:21, 258:3, 285:11, 285:19, 287:3, 288:16, 289:13, 289:19
industry-leading 289:20
infancy 55:21
infected 178:4, 182:2, 182:20, 183:12
infinitessimal 173:21
info 53:6
informed 239:17
infringement 243:12
ingres 134:15
inherent 246:3, 250:20, 251:1, 251:15, 251:17, 251:20
inherently 251:11
initiate 99:3, 151:13
inquire 143:9
inquiries 127:17
insecure 243:1
insert 95:20, 134:18, 136:6, 137:17, 137:18, 137:20, 138:20, 141:4, 141:6, 141:12, 141:17, 141:19, 143:7
inserted 136:17, 142:8
inserting 137:13, 138:14
insights 109:6, 186:21

install
46:12, 46:21, 50:2
instances
107:1
instant
162:16, 173:20
instead
58:6, 59:7, 60:10, 63:2, 84:9, 84:18, 85:22, 87:19, 262:16
instruction
173:22, 174:3, 174:4, 174:6, 174:18
instructions
174:18
integrity
142:11, 142:12, 142:21, 144:11
intelligence
187:1, 188:8
intensive
128:7
interest
257:22
interested
296:22
interesting
108:15, 109:12, 109:17, 110:3, 110:4, 110:19, 111:5, 111:14, 112:12, 113:1, 114:21, 115:8, 115:18, 116:8, 116:11, 117:15, 117:21, 118:6, 118:9, 119:4, 119:7, 119:21, 121:12, 185:6, 188:17, 189:4, 189:8, 194:15, 194:17, 223:12, 224:3, 224:4, 268:18, 270:7
internal
38:9, 45:22, 46:2, 81:1, 82:12, 87:16, 90:2
international
233:20
internet
178:4, 186:14, 242:22, 276:2
interpret
17:5, 17:14, 203:17, 246:17, 248:22, 249:6
interrupt
78:8
introduce
187:18
introduces
187:20
intrusion
39:11, 43:7, 52:16, 55:12, 56:7, 58:15, 64:4, 255:10
intrusions
55:17, 254:22
invalidity
243:13
invent
106:12, 111:22, 112:22, 116:15
invented
113:22, 124:12, 290:17
invention
123:16, 199:5, 268:22
inventions
205:13
inventor
28:11, 113:3, 283:6, 288:22
inventors
106:11, 111:21, 112:21, 113:22, 116:14, 122:12, 124:12, 266:17, 266:22
involved
184:16, 236:16
involves
281:21
ip
192:2, 192:18, 192:19, 208:6, 208:9, 208:10, 211:9, 212:15, 212:16, 212:19, 212:21, 213:7, 213:11, 214:10, 215:2, 215:4, 236:21, 237:1, 237:7, 237:9, 237:10, 237:16, 237:20, 238:4, 238:5, 238:7, 238:10, 238:14, 238:16, 238:17, 292:6, 292:9, 292:10, 293:11
ipr
1:6, 5:13, 54:3, 54:5, 204:18, 215:13, 235:6, 235:11, 235:12, 254:15, 259:10
ipr-
204:19, 205:9, 235:10
ips
237:18
irrelevant
188:14
isolate
114:7
iss
53:9, 65:13, 66:1, 66:6, 66:15, 70:2, 70:3, 76:5, 77:5, 77:14, 78:13, 78:14, 78:19, 79:11, 87:16, 88:22, 89:6, 92:4, 93:5, 93:12, 94:21, 95:3, 96:18, 98:21, 99:1, 99:20, 101:13, 101:20, 101:22, 258:11, 258:12, 273:15
iss's
65:16
issue
53:7
italicize
251:14
itself
138:5, 184:4, 220:20, 225:12, 237:8, 238:5, 238:15, 238:17, 241:17

J

job
1:20, 44:11, 63:13, 63:17, 63:19, 111:14, 111:16, 118:11, 148:22
jobs
63:21
jonathan
3:3, 5:8, 11:9, 83:2, 102:17, 150:14, 202:21, 255:17
jumped
25:6
junk
98:2

K

keep
40:8, 46:14, 60:18, 76:14, 95:11, 95:19, 96:6, 96:8, 196:11, 218:18
kept
154:1

kessler
3:5
key
125:20
keyword
98:1, 286:7
keywords
196:5
kickback
218:18
kind
43:19, 63:20, 82:10, 104:11, 109:4, 109:6, 110:10, 110:15, 110:20, 111:18, 113:11, 127:2, 128:7, 134:15, 140:5, 140:6, 152:19, 159:20, 169:3, 183:14, 183:17, 183:21, 186:7, 187:14, 188:5, 192:22, 193:2, 216:16, 233:16, 234:20, 248:15, 269:13, 271:8
kinds
71:2, 157:6, 179:10, 206:4
knew
284:21
knowing
182:17
knowledge
7:22, 73:22, 92:22, 186:19, 188:11
known
42:17, 42:18, 42:21, 42:22, 44:9, 49:5, 49:15, 54:13, 54:21, 55:11, 55:14, 56:18, 57:5, 69:18, 72:11, 77:10, 98:14, 111:10, 113:2, 113:13, 113:17, 113:21, 121:14, 122:11, 122:19, 123:5, 123:8, 123:13, 125:4, 125:11, 125:12, 125:15, 126:12, 126:14, 126:17, 180:18, 183:18, 183:22, 184:3, 184:4, 184:15, 184:22, 191:11, 191:16, 224:4, 231:18, 232:21, 252:21, 254:16, 254:20
knows
91:12, 189:15, 237:8
kosher
149:6

L

language
9:3, 13:10, 17:11, 179:18, 199:8, 203:17, 239:8, 243:5, 281:2, 293:1
languages
279:9
large
132:13, 258:13, 275:20
largely
275:19
last
5:16, 19:11, 31:13, 40:14, 45:4, 50:14, 54:11, 54:19, 65:22, 70:14, 71:19, 79:13, 84:8, 103:4, 168:5, 175:16, 224:12, 251:5, 254:18, 257:7, 268:4
lasts
164:3
late
29:13, 40:12, 43:1, 43:18, 48:2, 48:15, 48:16, 49:17, 50:21, 51:8, 51:12, 56:18, 56:21, 59:2, 69:19, 70:2, 233:17
later
36:19, 166:17, 170:18, 201:21, 207:13
latter
128:22
laugh
35:21, 168:5
layer
182:4
lays
226:19
leader
65:14
leap
180:12
learn
242:7
learned
140:19
learning
233:14
least
9:5, 31:17, 40:18, 40:19, 42:10, 45:1, 48:6, 64:14, 72:20, 75:11, 76:8, 79:9, 97:9, 126:7, 184:5, 184:17, 228:15, 276:15
leave
186:8
lee
1:13, 2:1, 4:4, 5:8, 51:6, 51:7, 106:3, 151:1, 212:2, 212:4, 259:6, 291:13, 291:15, 295:2, 296:5, 296:14
left
8:7, 8:12, 13:16, 13:17, 122:11, 123:12, 123:18, 123:22, 124:11, 125:14, 125:19, 126:2, 267:2
left-hand
43:12
leftover
37:7, 124:8, 124:9, 124:17
let's
6:20, 24:3, 24:6, 26:4, 42:16, 50:15, 56:14, 57:16, 57:18, 61:12, 65:9, 93:4, 94:10, 96:11, 97:10, 99:2, 102:15, 114:6, 139:14, 140:21, 145:14, 146:17, 150:16, 151:10, 152:3, 153:9, 157:14, 159:2, 169:11, 172:14, 186:8, 192:20, 193:22, 200:9, 211:14, 213:5, 219:22, 234:5, 234:15, 237:7, 239:1, 244:12, 244:19, 259:2, 268:9, 273:13, 274:21, 281:8, 285:7, 287:18, 287:20
level
9:8, 9:20,

10:1, 10:5, 10:7, 10:12, 10:13, 10:18, 11:2, 11:7, 11:14, 12:4, 38:16, 174:6, 179:6, 257:11, 275:6, 276:18, 277:1, 277:6, 278:5, 278:8, 278:9, 278:13, 278:16, 279:17, 279:18, 279:19, 280:2, 280:5, 280:8, 280:9, 280:10, 280:22, 281:2, 281:13, 282:4, 282:7, 282:16, 282:18, 282:21, 283:10, 283:21, 285:3
life
138:8
light
245:14
likely
40:9, 40:20, 69:12, 69:15, 77:9, 110:4, 116:10, 118:9, 194:17, 267:1, 268:19
likewise
79:11, 271:22
limit
198:7, 222:6, 223:6
limitation
12:14, 13:5, 22:20, 23:3, 24:2, 25:11, 27:14, 27:19, 30:13, 31:16, 31:17, 32:11, 99:8, 193:21, 198:1, 221:20, 228:8, 240:1, 250:7, 271:15, 279:7
limitations
17:9, 23:11, 25:12, 31:9, 33:13, 33:20, 224:15, 224:16, 224:22, 243:11, 269:18, 277:8
limited
177:6, 201:12, 201:14, 202:4
line
108:10, 109:10, 110:14, 111:3, 114:10, 115:6, 117:13, 118:5, 119:19, 157:19, 158:14, 188:21, 240:2, 241:9, 241:10, 255:18, 290:3, 292:3, 293:18
lines
34:21
linking
240:21
list
30:10, 125:2, 125:3, 237:17, 238:17, 238:19
listed
57:7
listen
206:9
listing
125:8, 125:9
literally
258:19
little
146:9, 221:8, 221:19, 222:20, 226:12, 243:9, 267:15
live
138:9
lived
181:9
llp
2:5, 3:13, 296:15
loaded
132:12
loading
161:14, 184:1
local
59:9
locally
73:21
locate
62:18, 63:14, 216:2
located
100:3
location
100:19, 101:2, 101:3, 101:6
lock
138:19, 138:21, 139:21, 141:17, 142:14, 142:16, 142:20, 143:8, 143:10, 143:13, 143:16, 143:20, 144:10, 144:11, 145:6, 146:16, 147:10, 148:21, 148:22, 149:1, 149:4, 149:8, 150:1, 150:5, 150:6, 150:7, 150:10, 152:16, 152:20, 154:21, 155:3, 155:4, 163:17, 164:3, 164:5, 164:14, 164:17, 164:19, 165:1, 167:3, 167:10, 168:4, 168:12, 168:16
locked
146:12, 147:1, 148:14, 149:17, 152:6, 152:13, 168:1, 168:13, 173:3, 173:7
locking
138:16, 139:4, 140:5, 141:2, 142:4, 142:22, 143:6, 150:5, 150:9, 152:15, 166:22, 168:19, 173:5
log
75:18
logged
103:16
long
48:14, 144:16, 147:8, 163:7, 166:20
longer
166:13
look
6:20, 8:18, 9:3, 19:10, 24:6, 26:4, 29:20, 51:20, 55:6, 57:18, 59:6, 61:10, 62:9, 62:10, 63:17, 63:18, 65:9, 66:12, 68:6, 72:15, 73:21, 76:2, 77:1, 78:3, 81:1, 81:17, 81:21, 82:6, 87:20, 90:21, 92:3, 93:9, 93:12, 93:19, 94:12, 94:22, 98:22, 102:11, 106:6, 108:20, 109:22, 110:16, 131:21, 135:11, 138:15, 157:14, 176:5, 179:15, 179:20, 180:21, 181:4, 181:5, 185:3, 188:7, 194:21, 195:13, 196:3, 197:19, 203:21, 205:22, 206:5, 212:12,

212:19, 215:22, 218:19, 226:8, 226:10, 227:14, 231:17, 232:19, 234:12, 241:5, 246:12, 246:21, 249:14, 255:7, 256:15, 257:6, 257:14, 258:2, 258:8, 260:4, 261:20, 263:10, 264:8, 267:22, 285:5, 287:14
look's
206:5
looked
102:15, 124:21, 125:1, 212:14, 247:1, 247:5
looking
25:7, 57:6, 70:20, 93:21, 109:1, 109:8, 112:8, 112:11, 114:4, 135:6, 176:11, 179:13, 195:7, 195:9, 196:9, 196:11, 211:2, 216:11, 257:4, 258:1, 258:18, 258:19, 262:2, 262:18, 270:9, 273:11
looks
203:4, 204:12, 205:14, 207:20, 208:15, 208:19, 209:2, 210:7, 210:15, 215:14
lot
41:3, 41:21, 71:1, 74:2, 99:17, 110:6, 129:4, 131:5, 131:18, 131:19, 132:16, 133:1, 134:21, 135:9, 136:3, 148:18, 155:15, 174:13, 179:1, 182:7, 188:7, 237:6, 242:13, 257:20, 258:4
love
130:7, 131:21, 234:21
lower
238:3
lunch
150:18
luncheon
150:21

M

machine
183:12, 183:19, 184:22, 185:2, 186:13, 186:15, 233:14
main
86:3, 276:14, 276:15
mainly
275:4
mainstay
276:11
maintain
58:16
make
46:14, 46:21, 47:1, 47:14, 77:12, 93:15, 131:3, 137:1, 152:4, 175:5, 180:13, 203:19, 204:22, 205:2, 232:9
makes
47:8, 75:21, 110:5, 224:15, 231:12, 233:1
making
47:6, 47:10, 47:20, 48:3, 48:21, 214:21
malicious
184:16
malware
180:18, 181:12, 183:19, 183:20, 192:20
manage
45:22, 46:13, 46:21, 59:7, 60:14, 72:19, 72:20, 72:22, 74:5, 99:9, 99:10, 127:15, 159:5, 251:8, 253:9
managed
7:17, 8:2, 8:20, 17:20, 18:3, 18:6, 18:9, 19:4, 29:9, 42:5, 51:21, 55:20, 56:3, 56:16, 56:17, 60:21, 70:1, 253:6, 253:15, 253:17, 271:17, 275:3, 286:7, 286:11, 287:21, 288:4, 288:5, 288:11, 289:4, 289:7, 289:21
management
8:20, 138:13, 149:10
managing
59:8
manual
80:22
manually
158:3
manuals
46:19
many
81:19, 83:10, 83:11, 85:16, 88:21, 106:22, 109:13, 111:6, 135:2, 157:3, 165:2, 166:4, 173:21, 234:13, 271:7, 276:5
mapping
229:2, 229:15
marked
4:11, 37:21, 52:15, 54:2, 216:21
market
65:14, 275:18
marketing
191:3
markets
275:20
marriage
296:20
match
42:16, 42:17, 43:12
matched
196:6, 215:5
matches
39:17
matching
40:16, 216:19, 231:21
material
178:7, 178:16, 185:11, 186:1, 186:6
materials
180:2, 180:6, 181:19
matter
81:2, 297:1
maybe
10:14, 42:15, 46:7, 52:14, 63:22, 73:10, 73:11, 73:12, 81:18, 105:21, 122:5, 124:7, 126:16, 157:9, 165:14, 168:8, 183:21, 202:14, 227:14, 235:2, 258:12, 260:11, 262:15, 264:18

meaning
14:20, 23:16, 39:6, 40:14, 42:20, 55:11, 60:12, 68:15, 97:19, 110:1, 116:9, 127:1, 134:21, 135:2, 142:8, 147:10, 149:3, 149:4, 167:3, 169:21, 172:10, 173:22, 177:3, 183:11, 183:21, 184:21, 189:20, 190:4, 194:16, 237:5, 278:21, 280:3, 281:10, 281:21, 282:15, 289:3
meaningful
124:18
meanings
200:2
means
11:16, 14:19, 39:7, 48:22, 50:4, 68:14, 69:10, 97:22, 109:12, 111:4, 112:12, 113:9, 114:19, 114:21, 118:3, 118:5, 124:3, 127:3, 128:22, 138:1, 142:4, 143:6, 143:14, 145:3, 145:7, 147:18, 152:13, 155:11, 155:12, 156:12, 173:20, 180:11, 188:22, 189:1, 189:3, 200:1, 203:12, 203:13, 204:10, 218:4, 223:11, 223:12, 225:8, 232:18, 238:4, 238:17, 241:13, 251:9, 251:20, 277:18, 277:20, 286:21, 288:6, 289:22, 292:11, 292:13, 292:14
meant
113:4, 195:6, 207:10, 215:17
measured
284:2
mechanism
62:6, 189:19, 189:20, 190:6, 214:22, 215:8
mechanisms
48:1
meet
5:9, 23:10, 228:7, 243:11, 265:15
meeting
224:14, 224:21
meets
17:8, 23:3, 25:11, 26:8, 26:21, 26:22, 27:4, 30:13, 31:9, 32:1, 32:7, 33:13, 33:20, 34:6, 36:9, 45:13, 227:9, 270:22, 271:15
member
257:13
memory
58:20, 124:18, 126:6, 129:1, 129:10, 129:12, 129:14, 129:16, 130:21, 132:12, 135:4, 135:5, 137:8, 137:10, 161:22, 171:6, 171:20, 172:2, 172:6, 172:8, 226:22, 236:1, 246:13, 263:11
mention
286:6, 288:13
mentioning
52:12
mentions
84:7
mess
141:2
message
82:16, 160:5, 168:7
messages
38:7, 292:5
met
262:6, 278:6
method
24:18, 24:21, 25:20, 27:12, 27:18, 233:16
microsoft
127:5, 127:8
mid
44:20, 276:13
middle
35:1, 175:2, 193:10
might
159:12, 224:1, 234:3, 234:4, 278:4
military
275:19
millions
38:7
mind
224:7
mine
157:4, 246:11
minimize
169:4
minute
246:5
mischaracterizes
26:12, 32:20, 41:15, 44:4, 49:3, 59:22, 63:8, 73:3, 86:12, 87:7, 100:21, 120:6, 130:5, 130:17, 136:20, 149:20, 157:1, 183:6, 185:15, 192:14, 202:7, 204:6, 204:15, 232:1, 238:13, 250:1, 256:4, 269:21, 294:7
mischaracterizing
36:16
misquote
78:7, 78:8
misquoted
77:20
misreading
279:22
miss
78:7
missed
77:21
misstates
16:8, 16:22, 22:15, 32:2, 119:17, 171:1, 178:19, 215:19, 269:20, 283:13, 288:19
mm-hmm
53:5, 53:13, 58:3, 88:14, 103:15, 111:8, 123:9, 133:4, 145:19, 146:1, 146:20, 219:14, 219:17, 220:8, 226:17, 260:3, 260:13, 261:10, 261:15, 266:20, 275:9, 285:17, 291:10
mode
48:9, 48:10, 209:10
modern
170:7
modification
45:14, 49:16

modified
49:1
modify
192:9, 289:15
modifying
45:15, 47:4, 48:4, 155:11, 155:12, 163:16, 163:20, 163:22, 165:3, 170:17, 279:12
module
33:18, 211:10, 213:18
modules
152:18, 209:22
moment
163:2, 163:10, 163:13
money
140:4
mongodb
134:16
monitor
62:7, 81:18, 82:5, 186:18, 213:12, 272:3, 272:7, 293:3
monitored
9:5, 234:18, 236:8, 272:10
more
8:15, 24:1, 39:4, 39:13, 58:14, 59:13, 82:11, 102:20, 117:1, 122:18, 133:11, 164:3, 165:20, 170:11, 174:12, 196:8, 196:11, 239:8, 248:11, 250:3, 258:8, 261:20, 281:11, 281:16, 294:17
morning
5:8
most
60:9, 69:12, 69:15, 70:14, 75:21, 114:13, 126:21, 183:8, 222:15, 223:16, 224:7, 231:11, 232:9, 233:1, 233:19, 274:15
motivation
72:20
mouth
95:7, 95:12
moving
45:4
msm
18:12, 18:16, 18:20, 19:6, 19:12, 19:16, 20:1, 20:15, 21:18, 21:21, 22:11, 22:22, 23:2, 23:11, 23:21, 24:13, 25:10, 25:19, 25:21, 26:2, 26:8, 26:15, 26:21, 27:4, 27:8, 27:12, 27:21, 28:2, 28:4, 28:14, 28:15, 28:18, 28:21, 29:3, 29:8, 30:1, 30:5, 30:13, 30:19, 31:5, 31:9, 31:14, 32:1, 32:14, 32:18, 33:1, 33:4, 33:7, 33:13, 33:20, 35:7, 36:18, 37:6, 37:15, 38:1, 41:17, 43:21, 45:13, 51:7, 51:11, 51:16, 61:7, 267:4, 267:8, 267:17, 268:5, 269:4, 270:22, 271:15, 275:2, 275:7, 276:17, 276:20, 280:3, 280:4, 280:18, 281:1, 282:5, 282:6, 282:20, 283:1, 283:6, 283:9, 284:1, 285:12, 285:20, 286:17, 287:4, 288:7, 289:1, 289:5, 289:14, 290:2, 290:5, 290:6
much
43:5, 44:6, 47:18, 71:15, 88:2, 88:5, 166:3, 167:1, 167:11
multi-stage
244:14, 244:18
multiple
39:15, 80:20, 82:14, 102:3, 118:22, 121:17, 130:18, 134:9, 136:21, 151:7, 151:11, 151:16, 151:18, 151:19, 152:2, 155:17, 158:16, 158:17, 159:4, 160:12, 165:11, 167:20, 168:21, 169:18, 170:10, 174:17, 200:8, 206:4, 206:7, 206:13, 209:10, 228:14, 232:3, 232:4, 237:5, 244:9, 245:4, 258:14, 268:14, 274:1, 274:6, 277:8, 284:9, 286:15
multistage
263:21, 264:4, 264:6, 265:5, 265:6, 266:9, 277:9, 281:22
must
71:21, 84:13, 220:6, 293:20, 293:21, 294:9
myself
73:21, 88:7
mysql
127:7, 127:8, 127:21, 131:12

N

name
33:12, 33:19, 214:1
names
33:18
narrower
178:8
natural
40:7, 41:11, 119:13, 120:2, 120:14, 120:22, 121:4
nature
123:16
necessarily
88:12, 187:8, 189:8, 189:9, 242:14
necessary
171:5, 251:22, 288:14, 288:15
need
21:12, 24:1, 29:16, 39:14, 57:15, 92:3, 93:12, 94:12, 94:22, 117:19, 133:11, 135:11, 143:20, 164:14, 168:9, 198:8, 206:8, 236:2, 237:16, 238:6, 242:14, 243:13, 246:12, 248:11, 250:2, 251:11,

252:1, 252:10, 293:2
needs
38:17, 75:10, 160:1, 169:20, 198:12
negative
37:6, 40:6, 42:14, 44:1, 59:10, 108:12, 110:1, 112:19, 114:3, 114:7, 114:18, 115:7, 115:17, 116:7, 116:16, 117:6, 117:14, 117:18, 119:3, 119:14, 119:20, 120:3, 120:9, 120:15, 120:22, 121:21, 122:10, 123:7, 123:11, 124:10, 125:12, 140:16, 179:10, 189:1, 189:16, 194:14, 194:22, 195:1, 200:2, 200:10, 203:11, 210:17, 213:6, 214:18, 220:13, 223:11, 232:8, 232:21, 267:9, 267:18, 268:18, 269:6, 270:1, 270:6, 270:18
negatively
41:13, 199:10, 203:6, 204:1, 205:16, 206:1, 267:10, 267:20, 285:21, 286:1, 287:5, 287:7
neighborhood
184:22
neither
35:13, 107:8, 115:6, 115:17, 117:14, 119:19, 120:9, 120:19, 125:4, 194:7, 199:18, 199:22, 202:2, 202:10, 267:9, 267:19, 285:22, 287:6
net
52:7, 52:12, 57:16, 75:18, 79:2, 80:12
netranger
53:9, 57:19, 58:6, 61:3, 65:17, 72:17, 73:5, 76:5, 78:13, 78:14, 79:3, 79:14, 93:11, 94:22, 98:22, 99:1, 247:6, 247:11, 247:18, 249:12, 250:11, 253:3, 253:13, 254:10, 255:1, 255:20, 273:21, 276:13, 282:9, 282:11
netranger's
80:22
network
7:4, 9:6, 24:15, 27:10, 34:12, 35:2, 36:20, 38:8, 39:9, 51:8, 51:11, 51:17, 52:3, 53:10, 55:13, 56:6, 58:8, 58:15, 61:14, 61:22, 63:6, 63:18, 64:21, 65:15, 66:8, 66:19, 68:1, 68:7, 68:12, 76:21, 78:16, 83:8, 85:6, 88:10, 92:13, 93:1, 93:21, 94:1, 97:13, 98:5, 110:8, 176:7, 183:3, 184:11, 211:10, 213:18, 214:10, 234:19, 236:8, 236:10, 237:15, 238:5, 239:19, 253:9, 255:10, 268:11, 269:16, 272:18, 273:14, 273:17, 275:18, 276:3
networks
1:4, 25:17, 273:2
never
28:17, 28:20, 78:2, 78:3, 78:22, 79:1, 79:8, 79:16, 80:1, 95:10, 95:18, 144:22, 186:6, 188:13, 193:15, 265:12, 282:22, 283:1
new
1:14, 2:7, 2:12, 3:6, 3:15, 10:3, 57:2, 66:3, 66:8, 66:19, 70:13, 70:19, 71:4, 71:5, 72:5, 72:7, 72:12, 76:10, 84:11, 84:12, 85:4, 85:5, 86:4, 86:9, 86:20, 87:4, 88:19, 89:11, 90:12, 101:9, 114:5, 116:22, 117:2, 121:18, 122:3, 160:17, 161:8, 200:4, 200:5, 200:12, 218:13, 258:18, 275:2, 276:1, 281:9, 296:3, 296:15
newly
219:4
next
37:1, 42:1, 46:11, 65:10, 101:10, 162:19, 163:18, 169:13, 180:4, 180:8, 196:1, 218:19, 220:10, 245:22, 246:4, 261:11, 270:11, 276:1, 292:14
nice
5:9
nicely
39:22
nobody
138:17, 138:19, 139:21, 140:12, 142:5, 142:18, 143:6, 145:7, 155:4, 182:21
node
103:12
nolan
3:11, 82:7, 139:13, 139:14, 139:15, 139:18, 139:22
non-interesting
223:13
non-zero
186:11, 187:20, 188:1
none
62:19, 85:1, 134:3, 152:13, 152:16, 246:1, 250:16, 250:18, 252:3, 277:4
nonobjectionable
180:1
noran
139:17
normal
40:8, 40:17,

40:18, 42:12, 42:16, 44:7, 231:17, 232:19, 233:15, 234:7
normally 38:22, 127:4, 127:14, 135:14, 145:2, 148:19, 149:6, 150:3, 162:3, 164:3, 180:15, 180:19, 180:20, 183:9, 184:15, 184:19, 189:20, 234:6, 237:13
nose 53:2
notarial 297:3
notary 2:11, 5:4, 296:2
note 182:9, 195:3, 245:12
noted 294:19
nothing 6:3, 6:7, 6:9, 47:2, 59:4, 59:17, 61:3, 62:10, 70:17, 75:17, 77:6, 80:7, 84:21, 156:15, 162:5, 167:4, 186:15, 250:8, 250:10, 293:2, 293:3
notified 80:10
notify 58:11, 60:8, 62:15, 63:12, 65:5, 77:5, 79:6, 79:21, 80:19, 83:16, 273:8
notion 173:5, 182:11
novel 56:5, 122:16, 126:6, 205:12, 255:9, 255:11, 284:10
novelty 269:10, 270:15
nuance 174:12
nuanced 258:9
nuances 257:21, 258:4
number 6:12, 73:21, 103:11, 168:8, 182:17, 217:1, 275:16, 276:7, 288:3
nw 3:6
ny 2:7, 3:15, 296:16

O

oath 89:19
object 23:8, 32:19, 55:7, 78:11, 82:8, 95:21, 96:20, 102:9, 188:6, 212:9, 236:18
objecting 36:6
objection 6:5, 7:2, 7:13, 7:18, 9:11, 9:22, 10:9, 10:20, 11:8, 12:13, 12:19, 13:8, 14:9, 15:19, 16:7, 16:14, 16:21, 17:12, 17:22, 18:4, 19:1, 19:8, 20:3, 20:11, 21:2, 21:9, 21:19, 22:14, 23:4, 23:12, 24:10, 25:13, 26:11, 27:6, 28:6, 30:2, 30:7, 30:15, 31:11, 32:2, 33:5, 33:9, 33:15, 33:22, 35:15, 37:9, 37:17, 41:14, 44:3, 45:18, 49:2, 52:5, 52:10, 53:16, 55:3, 56:20, 57:13, 58:22, 59:21, 61:16, 62:3, 63:7, 64:22, 66:10, 66:21, 67:18, 69:7, 69:20, 70:7, 70:21, 71:13, 72:1, 72:8, 72:16, 73:2, 73:16, 74:14, 75:13, 76:12, 78:20, 80:2, 80:17, 81:6, 81:14, 83:1, 84:6, 84:15, 85:7, 85:14, 86:11, 87:6, 88:20, 89:12, 89:22, 90:1, 90:8, 90:13, 94:2, 96:17, 97:7, 97:15, 98:9, 99:21, 100:4, 100:10, 100:14, 100:20, 101:7, 101:14, 102:12, 103:7, 104:1, 104:8, 104:17, 105:9, 106:16, 106:21, 107:17, 116:2, 116:18, 118:1, 118:18, 119:16, 120:5, 120:16, 121:16, 124:14, 125:16, 126:19, 128:18, 130:4, 130:16, 131:16, 134:13, 136:7, 136:19, 141:15, 142:1, 143:2, 144:1, 144:15, 144:21, 146:5, 146:13, 147:2, 148:16, 149:19, 151:8, 152:10, 153:6, 154:17, 155:13, 156:22, 158:9, 159:17, 160:19, 161:10, 164:1, 164:11, 165:6, 165:22, 166:6, 167:16, 169:9, 171:1, 172:3, 173:19, 175:15, 176:3, 177:21, 178:10, 178:19, 181:14, 183:5, 184:13, 185:14, 186:3, 188:19, 189:11, 190:19, 191:17, 192:13, 197:6, 197:11, 199:11, 201:16, 202:6, 203:8, 204:5, 204:14, 205:4, 205:19, 208:1, 209:15, 210:13, 215:18, 215:19, 217:13, 217:20, 218:11, 221:11, 221:22, 222:9, 227:12, 228:11, 229:7, 230:5, 231:22, 232:16, 237:3, 238:12, 240:17, 243:16,

244:7, 245:21, 246:9, 246:18, 247:16, 248:9, 249:1, 249:22, 251:19, 253:19, 255:4, 256:3, 256:10, 256:17, 257:17, 265:21, 267:12, 269:20, 272:12, 273:3, 274:12, 277:7, 278:7, 279:21, 280:16, 283:3, 283:13, 284:4, 286:2, 287:8, 288:18, 289:17, 293:16, 294:6, 294:16
objectionable
179:22, 180:6, 180:9, 180:17, 191:21, 192:4, 193:4, 193:5
objections
14:18, 60:5, 91:6, 121:2, 168:3
obscene
178:7, 178:16
obvious
42:14, 43:22, 82:19, 83:7, 86:5, 116:7, 116:13, 129:20, 208:12, 210:3, 223:16, 251:7, 258:7, 284:20
obviously
50:15, 176:8, 251:15
obviousness
245:14
occupy
42:13
occur
85:13
occurred
74:13, 296:14
occurring
170:4, 170:19
occurs
174:11, 259:18
odd
181:4
offend
96:7
offer
28:13, 31:5, 31:12, 36:4, 36:9, 89:14, 92:9, 92:15, 93:3, 109:2, 235:4, 263:6, 263:16, 271:6
offered
11:21, 32:5, 34:2, 52:8, 53:20, 57:11, 58:21, 60:2, 229:10, 230:9
offering
17:5, 17:7, 17:17, 59:3, 66:6, 92:7, 92:20, 250:6, 262:5
offerings
65:16
offers
58:5
office
1:1
offices
2:2, 296:14
offline
126:18, 158:3, 159:13
oh
7:6, 62:17, 63:17, 82:16, 112:5, 119:2, 129:9, 135:6, 135:10, 138:8, 140:9, 160:1, 168:15, 174:4, 181:6, 182:16, 182:22, 184:7, 185:5, 192:8, 212:19, 235:8, 237:7, 237:14, 238:16, 248:16, 249:10, 249:14, 249:17, 252:15
old
14:19
older
282:12
once
103:5, 108:11, 144:18, 208:5
one
8:22, 9:5, 20:15, 20:19, 22:6, 22:12, 26:4, 29:20, 38:14, 51:15, 52:6, 67:6, 72:20, 82:9, 90:5, 100:6, 101:20, 125:6, 125:7, 127:6, 128:14, 129:8, 129:9, 130:12, 130:21, 138:6, 144:13, 151:5, 152:14, 153:1, 153:5, 154:8, 154:14, 156:5, 158:19, 160:9, 160:10, 162:14, 162:17, 163:2, 163:5, 163:10, 165:20, 166:12, 166:16, 169:11, 170:8, 170:11, 170:12, 172:18, 172:21, 173:12, 173:22, 174:20, 182:14, 184:17, 190:4, 196:22, 197:1, 205:12, 212:16, 215:5, 222:2, 222:22, 236:20, 236:22, 237:11, 237:12, 243:14, 247:1, 248:7, 251:14, 258:1, 258:4, 258:14, 276:8, 276:14, 276:16, 282:11, 283:15
ones
214:20, 252:22
online
128:2, 128:11, 128:17, 130:3, 130:15, 131:14, 132:5, 133:9, 134:1, 134:7, 134:19, 136:6, 136:18, 137:22, 138:1, 156:20
only
20:19, 21:12, 29:20, 47:21, 51:8, 51:11, 51:15, 65:3, 67:9, 79:5, 83:13, 84:7, 87:11, 88:5, 101:20, 125:7, 139:9, 142:14, 157:11, 162:14, 162:17, 163:2, 164:12, 168:15, 168:16, 170:8, 170:12, 172:12, 172:20, 173:12, 173:22, 174:20, 184:14, 195:20, 214:17, 214:18, 218:20, 223:8, 224:3, 229:10, 256:22, 259:16, 262:12, 265:14, 281:7, 293:12
open
178:3, 195:21, 196:10, 217:22, 218:1, 218:14, 218:17, 219:16, 219:18, 219:20,

219:21, 291:20, 291:21, 292:12, 292:15, 292:21, 292:22
opened
195:19, 218:21, 219:4, 292:14
opens
292:8, 293:10
operate
140:15, 153:12, 254:12, 257:21
operates
81:17, 143:19, 173:22
operating
6:21, 17:20, 18:3, 24:14, 25:16, 27:9, 138:2, 140:19, 143:22, 154:7, 154:12, 156:13, 174:15, 176:6, 211:11, 213:16, 213:18, 213:20, 214:9, 215:3, 216:14
operation
8:11, 8:17, 16:2, 45:16, 97:1, 97:11, 132:13, 145:4, 158:4, 158:6, 167:1, 167:2, 167:11, 173:17, 174:11, 188:15, 244:16, 244:17, 257:20, 264:1, 284:17
operational
241:1
operations
38:15, 58:8, 94:17, 98:1, 98:6, 242:21, 244:21, 248:14, 250:5, 256:20, 258:13, 265:8, 266:11
opine
11:3, 11:4, 17:15, 51:20, 75:3, 79:9, 80:7, 80:21, 82:18, 83:13, 85:2, 87:14, 87:19, 89:7, 89:8, 90:16, 91:18, 105:19, 107:20, 107:21, 123:1, 128:13, 130:10, 131:6, 131:7, 131:22, 132:1, 133:12, 133:19, 135:20, 136:14, 157:11, 246:22, 250:5, 254:9
opined
11:16, 179:3
opining
82:11, 89:1
opinion
10:8, 10:16, 10:17, 11:13, 11:17, 11:18, 17:17, 19:16, 20:1, 21:13, 21:16, 22:13, 22:22, 24:4, 25:21, 26:2, 28:13, 29:18, 30:22, 31:4, 31:12, 31:18, 32:5, 32:9, 34:3, 35:20, 36:5, 36:9, 53:20, 53:22, 56:12, 60:20, 63:14, 87:9, 88:11, 89:14, 90:5, 92:7, 92:15, 92:19, 93:3, 133:13, 136:2, 169:5, 229:11, 230:8, 230:9, 230:14, 230:15, 249:20, 261:17, 262:5, 263:7, 263:16, 266:5, 266:6, 269:15, 280:7, 282:14, 283:19, 285:6, 289:10
opinions
10:22, 17:6, 17:7, 28:5, 29:1, 34:8, 92:9, 92:20, 205:2
opportunity
50:5
opposite
182:20
optimize
167:20, 168:21
option
294:4
options
46:18
oracle
127:19, 128:10, 128:16, 130:1, 131:6, 131:12, 134:15, 134:17, 136:4, 136:17
order
29:17, 80:16, 81:11, 93:20, 104:13, 104:19, 105:7, 105:13, 105:17, 115:22, 148:7, 216:16, 217:16, 243:11
ordered
104:21
ordinary
38:21, 40:1, 64:2, 64:15, 66:17, 115:21, 117:9, 156:19, 175:20, 248:21, 249:5, 257:11, 257:16, 290:16, 291:1
org
94:13
organization
94:20, 189:21, 190:4, 190:10, 274:5
organizational-specific
94:8
organize
169:19
organized
92:4, 138:4, 168:13
os
215:10
other
27:3, 38:12, 38:20, 46:11, 46:13, 46:18, 63:22, 65:16, 71:21, 73:11, 74:7, 89:6, 90:6, 92:2, 112:7, 128:15, 129:8, 130:12, 136:10, 142:15, 143:17, 145:7, 150:8, 152:6, 152:7, 152:18, 153:3, 153:4, 153:9, 153:15, 154:6, 154:15, 155:5, 156:10, 156:15, 158:20, 179:15, 180:14, 186:7, 186:12, 186:20, 208:10, 208:11, 209:5, 209:22, 214:15, 214:19, 216:2, 233:6, 233:16, 234:12, 237:9, 243:15, 245:15, 245:18, 246:1, 246:7, 246:15, 248:8, 248:19,

249:3, 249:18, 250:15, 250:16, 250:18, 255:14, 264:14, 271:11, 281:6, 284:21, 285:3, 287:15
otherwise
11:15, 22:21, 24:4, 89:7, 92:6, 132:1, 133:12, 140:15, 218:14, 296:22
out
15:8, 24:20, 25:19, 27:12, 45:7, 52:14, 75:6, 86:9, 87:4, 88:18, 96:11, 100:12, 115:8, 117:15, 118:8, 119:21, 121:12, 121:13, 122:17, 129:8, 140:4, 143:12, 144:12, 152:6, 162:7, 162:8, 166:22, 169:11, 203:5, 203:6, 203:22, 204:1, 204:12, 205:15, 205:16, 205:22, 207:21, 207:22, 210:8, 210:17, 215:15, 216:1, 216:6, 216:13, 216:18, 224:16, 226:19, 260:11, 262:19, 264:8, 290:9, 290:19
outcome
296:22
outgoing
292:5
output
210:1
outside
10:10, 10:20, 12:19, 13:8, 14:9, 19:1, 19:8, 33:15, 33:22, 35:15, 35:17, 35:19, 36:1, 36:6, 55:7, 57:13, 58:22, 59:22, 61:16, 63:8, 64:22, 66:10, 66:21, 70:7, 71:13, 73:16, 74:14, 76:12, 78:20, 83:5, 84:16, 85:7, 85:14, 86:12, 87:7, 88:21, 89:12, 90:13, 94:2, 152:11
outsource
53:9, 59:16, 78:18, 78:19, 79:19
outsourced
247:6, 247:7
outsourcing
58:14
over
34:12, 35:3, 36:21, 40:4, 42:10, 43:6, 47:16, 59:12, 69:12, 69:15, 69:16, 73:8, 74:4, 75:15, 75:18, 75:22, 76:20, 88:9, 93:8, 94:11, 94:16, 95:9, 96:14, 97:5, 98:3, 99:7, 99:17, 99:18, 99:19, 104:10, 109:5, 109:8, 122:11, 123:12, 123:19, 123:22, 124:11, 125:14, 125:19, 126:2, 156:3, 166:13, 166:18, 217:12, 242:9, 242:22, 250:17, 260:4, 267:2, 268:3, 268:11, 269:17, 293:4
overall
59:9
own
11:13, 58:7, 58:17, 60:11, 63:3, 64:17, 67:13, 70:16, 72:22, 74:8, 74:20, 84:19, 85:22, 86:17, 87:22, 92:22, 133:15, 257:1
owner
1:10

P

p-i-n-g
160:4
pack
73:8
packet
236:13, 236:20, 273:13
packets
236:15
page
4:6, 5:16, 5:17, 18:18, 34:10, 34:19, 35:1, 37:22, 38:5, 39:3, 39:4, 41:10, 46:4, 46:5, 52:22, 54:15, 54:16, 54:17, 54:20, 57:7, 57:8, 57:18, 64:1, 66:1, 66:15, 71:20, 79:2, 79:14, 79:21, 83:19, 85:5, 97:9, 103:4, 125:6, 174:21, 175:2, 184:1, 193:7, 193:11, 195:14, 195:15, 196:1, 205:7, 220:11, 226:10, 227:5, 227:15, 228:16, 228:20, 229:1, 229:5, 235:13, 235:15, 235:17, 235:18, 235:21, 245:6, 245:8, 251:4, 256:1, 256:22, 259:11, 260:12, 260:14, 260:17, 260:19, 260:20, 261:11, 261:12, 262:1, 262:2, 262:10, 262:22, 264:9, 266:7, 271:1, 271:5, 271:6, 273:5, 275:16, 275:17, 285:7, 285:9, 290:13, 290:14
pages
1:21, 226:18, 227:4, 227:7, 227:11, 266:7, 271:11
pair
249:11
palo
1:4
panes
18:20, 25:15
papers
126:1
paragraphs
225:4, 262:3, 265:11, 265:17, 285:18, 286:3, 287:2, 287:11, 289:12
parallel
23:19, 163:7,

163:9, 165:16, 166:14, 166:19, 166:21, 170:13, 170:21
paren
25:19
parse
165:3
parsing
165:19
part
6:22, 7:3, 20:7, 24:14, 25:16, 27:9, 111:16, 118:11, 176:6, 215:10, 233:12, 264:5, 265:10, 265:13, 266:11, 270:17, 279:12
particular
24:2, 26:18, 36:10, 39:7, 49:5, 55:15, 69:10, 110:8, 141:3, 142:18, 144:10, 144:11, 145:12, 150:4, 153:1, 155:15, 157:12, 174:17, 192:19, 208:2, 233:14, 242:6, 251:5, 284:11, 292:9, 293:11
particularly
205:12
parties
296:19, 296:21
partners
73:19
parts
209:5
party
296:10
passed
8:14, 195:8
passes
254:1
passive
39:7
past
63:22, 73:10, 233:6
patents
42:17, 64:3, 181:6, 255:8
pattern
231:21
patterns
44:9, 112:9
pause
23:7, 132:15, 210:16
pay
46:12, 72:19, 182:5, 182:15, 288:10
payload
68:8
pdf
178:2
people
7:10, 28:14, 44:20, 49:20, 50:3, 50:7, 51:22, 72:18, 83:12, 112:7, 113:8, 114:10, 121:20, 121:22, 122:14, 124:2, 124:7, 124:9, 126:15, 135:9, 136:10, 141:1, 143:18, 150:2, 186:17, 187:6, 190:13, 233:19, 271:9, 288:10
percent
234:6
perform
117:1, 244:21
performance
284:2, 284:3
performed
9:20, 108:2, 231:6, 259:17, 267:3, 275:5
performing
265:5, 281:16
performs
9:9, 201:1, 244:17, 254:3, 269:6
period
83:13, 155:4, 166:13, 166:18, 169:7
permanent
127:1, 129:6, 129:17, 132:10, 132:11, 135:3
permit
270:9
perpetually
140:22
persistent
127:2
person
38:21, 40:1, 64:2, 64:15, 66:17, 92:12, 115:21, 117:9, 156:18, 175:20, 186:12, 190:18, 190:22, 248:21, 249:5, 257:11, 257:16, 290:16, 291:1
personal
47:11, 92:22
personally
29:11, 29:15, 29:17, 82:16, 134:2
personnel
63:5
pertaining
290:17
petition
52:11, 226:8, 226:18, 226:21, 227:3, 227:8, 227:11, 228:10, 229:2, 229:6, 229:15, 229:16, 230:2, 260:1, 260:4, 260:12, 260:14, 261:8, 261:13, 261:21, 262:9, 262:13, 262:18, 262:19, 264:9, 264:14, 265:19, 266:5, 266:6
petitioner
1:6, 3:2, 224:20, 245:12, 259:16, 261:22, 264:6, 265:12
petitioner's
175:3, 180:4, 229:9, 230:6, 251:6, 251:21, 252:9, 263:2, 290:18, 290:22
petitioners
224:13
ph
1:13, 2:1, 4:4, 5:2, 64:4, 232:4, 295:2, 296:5, 296:14
piece
184:18, 233:21
pilot
276:3
ping
160:2, 160:3, 160:5, 168:7
pipes
8:11, 13:20, 241:6, 241:8
place
40:4, 43:6, 84:7, 110:12, 159:4, 160:9, 182:1, 218:15, 234:10, 245:14
places
72:11, 85:16
plain
14:19

planning
58:12
please
15:6, 21:3, 197:12, 198:5, 198:8
point
6:8, 6:10, 10:4, 10:11, 11:9, 11:15, 12:14, 21:13, 29:10, 49:21, 67:6, 67:7, 71:3, 75:19, 76:18, 80:4, 93:4, 112:16, 118:10, 119:10, 119:11, 122:19, 122:20, 122:21, 145:6, 150:12, 150:15, 154:1, 155:3, 164:4, 166:22, 172:12, 177:15, 179:6, 179:17, 180:3, 181:2, 184:6, 186:9, 186:17, 187:8, 187:10, 187:11, 200:3, 200:14, 203:1, 206:2, 241:2, 243:2, 258:6, 258:13, 265:9, 266:1, 269:3, 271:8, 276:4, 287:2, 287:10, 288:5, 289:6, 289:11
pointed
41:6, 262:19
pointing
194:20, 199:9
points
122:17, 261:8, 261:13
policy
58:13, 189:20, 190:2, 190:5, 190:7, 190:10, 190:16, 190:20, 191:1, 191:4, 191:5, 191:6, 191:7, 191:9
pop
57:3
pops
81:20, 82:1
porn
177:18, 178:17, 179:14, 180:21, 181:18, 181:19, 182:1, 182:2, 182:13, 182:19, 182:22, 185:10, 185:12, 186:1, 186:5, 186:7, 187:9, 187:17
porno
182:10, 184:4, 184:7, 185:5, 188:13
pornographic
181:11
port
214:11, 292:9, 293:11
portal
46:9
portion
115:5, 218:9
posa's
239:15
pose
179:22, 180:3, 186:2
posita
40:1, 40:21, 42:11, 43:10, 43:15, 44:5, 60:16, 62:5, 62:13, 62:21, 63:1, 64:8, 69:9, 69:14, 74:18, 74:19, 77:7, 77:8, 82:13, 86:2, 86:5, 92:18, 94:4, 109:8, 109:14, 110:5, 110:6, 110:16, 110:22, 114:12, 118:6, 153:12, 175:5
position
35:22, 36:11, 210:2
positive
37:6, 40:6, 42:18, 43:22, 59:10, 108:4, 108:14, 108:17, 108:19, 109:2, 109:11, 109:16, 111:4, 111:10, 111:11, 111:22, 112:2, 112:6, 112:8, 112:11, 112:15, 112:17, 114:3, 114:8, 114:20, 115:8, 115:18, 116:8, 116:9, 116:15, 117:7, 117:15, 117:18, 118:3, 118:5, 119:15, 119:21, 120:3, 120:10, 120:14, 121:1, 122:1, 122:10, 123:5, 123:11, 124:11, 125:11, 179:11, 189:3, 189:17, 194:16, 195:1, 200:2, 200:10, 203:13, 213:6, 214:18, 220:13, 220:14, 223:12, 232:8, 267:8, 267:18, 268:20, 269:6, 270:1, 270:9, 270:18
positively
41:12, 117:22, 199:10, 203:5, 205:15, 205:22, 210:8, 215:15, 215:22, 221:9, 232:22, 267:10, 267:19, 285:21, 286:1, 287:5, 287:7
possible
103:17, 112:9, 142:15, 147:15, 155:22, 157:9, 157:10, 212:17, 272:1
possibly
79:21, 108:15, 109:12, 111:5, 112:12, 114:21, 117:17, 118:6, 189:3
post
122:22, 179:11, 187:4, 188:9, 199:20, 223:14, 231:1
post-filtering
9:10, 9:17, 35:12, 35:13, 37:2, 37:12, 37:13, 37:16, 38:2, 42:3, 44:14, 59:11, 99:11, 99:12, 107:7, 114:4, 114:6, 116:22, 117:2, 117:4, 122:18, 177:11, 179:12, 187:5, 188:10, 194:6, 194:7, 194:20, 195:3, 195:7, 199:17, 199:18, 200:12, 201:3, 201:9, 201:11, 201:14, 201:21, 202:9, 211:3, 213:4, 214:16, 220:5, 220:7, 220:15, 220:20,

220:21, 220:22, 221:4, 221:7, 221:14, 222:7, 222:11, 223:1, 223:6, 223:9, 225:6, 225:8, 225:9, 225:15, 228:17, 228:21, 229:4, 229:13, 230:1, 230:11, 230:13, 230:18, 231:3, 231:7, 231:10, 267:2, 269:2, 269:9, 270:13, 270:19, 281:8, 281:9, 284:12
postgres
134:15
potential
34:14, 35:4, 36:22, 45:7, 76:10, 150:1, 176:18, 186:10, 201:6, 236:17, 239:22, 268:12, 269:17
potentially
9:14, 12:11, 13:6, 14:6, 34:13, 35:9, 78:17, 103:22, 104:2, 104:5, 107:3, 109:17, 113:1, 155:19, 176:13, 176:19, 177:7, 177:9, 177:19, 177:22, 178:4, 178:6, 178:9, 178:13, 178:15, 178:17, 179:7, 185:11, 185:12, 186:2, 188:17, 194:3, 199:14, 201:6, 203:13, 270:10, 270:11, 272:16, 274:10, 294:4
practice
48:14, 52:1, 128:9, 129:21, 149:22, 150:4, 150:13, 188:2, 190:13
practiced
286:16
practices
286:21
practicing
129:20
praise
285:11, 285:19, 287:3, 288:10, 288:12, 288:16, 289:13
praised
286:10, 286:20, 286:22, 287:20, 289:8, 290:6
praises
286:5, 287:13, 287:16, 289:18
praising
289:8, 290:7, 290:10
preamble
24:17, 27:11
preferred
148:20, 158:2
present
45:8, 90:18
presented
45:8, 87:10, 89:15, 194:4
presenting
245:2, 248:1, 277:12
pretty
269:13
prevent
140:6
previous
38:12, 38:21, 210:6, 251:4
previously
26:14, 37:20, 52:15, 53:20, 210:5, 216:21
principle
111:20, 139:3, 140:17, 232:6
prior
16:22, 22:15, 26:12, 32:20, 49:13, 86:12, 87:7, 100:21, 119:17, 120:6, 130:5, 130:17, 136:20, 149:20, 157:1, 161:4, 161:12, 171:1, 178:19, 183:6, 185:15, 192:14, 246:15, 256:4, 269:21, 272:1, 272:8, 272:11, 272:19, 272:20
privacy
69:13, 74:8, 74:21, 274:7
probability
186:11, 187:21, 188:1
probably
18:14, 52:20, 94:9, 94:11, 129:1, 169:1, 266:2
probe
6:22, 7:3, 15:22, 16:16, 24:14, 25:16, 27:9, 45:16, 158:1, 159:3, 159:6, 159:12, 159:20, 160:10, 160:15, 160:17, 161:7, 161:8, 161:11, 165:5, 166:11, 167:14, 169:6, 169:8, 169:10, 169:19, 169:22, 170:3, 172:2, 172:4, 172:11, 176:6, 206:3, 208:6, 208:11, 209:6, 209:8, 209:9, 209:22, 241:6, 241:14, 244:15, 261:3, 261:8, 261:18, 262:20, 263:8, 263:18, 263:22, 264:2, 264:11, 265:7, 266:10, 267:3, 285:1
probe's
15:17, 169:14, 171:11
probes
9:1, 47:5, 171:6, 240:21, 253:22, 289:16
problem
8:19, 24:3, 27:15, 129:20, 131:20, 133:14, 135:8, 135:22, 136:12, 136:22, 137:3, 137:6, 137:12, 140:22, 148:3, 148:4, 150:1, 156:2, 156:21, 157:3, 157:8, 157:22, 158:8, 158:21, 159:5, 159:11, 160:14, 187:10, 191:11, 191:16
problems
155:19, 192:1, 192:12
proceed
219:21, 291:21, 292:17, 292:21
proceeding
5:14, 11:22, 54:5, 124:22, 204:19, 259:10
process
38:17, 94:18,

138:12, 220:5, 225:7
processed 95:16
processing 38:6, 42:10, 275:20
processor 170:13
produce 90:20
product 17:8, 18:16, 28:15, 33:18, 45:21, 45:22, 48:21, 48:22, 50:15, 53:2, 53:8, 59:7, 59:9, 65:10, 75:1, 111:18, 113:10, 114:15, 114:16, 131:22, 133:11, 247:6, 280:7, 280:9, 280:10, 280:11, 282:9
products 53:8, 73:19
program 45:6
programming 63:20
proofs 92:16
proper 154:4, 157:10, 188:8
proprietary 38:11, 41:8, 43:21
proskauer 2:5, 3:13, 296:15
protection 46:17
provide 55:13, 171:9, 231:6, 246:16, 248:20, 249:4, 249:21, 254:11, 264:21, 265:18, 282:15
provided 15:16, 61:13, 180:5, 258:22, 272:22, 273:15, 275:7, 276:19, 278:18, 280:3, 281:1, 282:5, 282:17, 282:18, 282:21
provider 59:16
provides 234:17, 236:7, 236:9, 248:6, 254:3, 281:19
public 2:12, 5:4, 296:1, 296:3
publicly 29:2
publish 233:18
pull 144:12
purported 259:17
purpose 24:9, 25:9, 72:13, 76:19, 118:9, 118:10
purposes 77:1, 149:2, 176:10, 193:1
put 8:6, 18:17, 43:2, 56:11, 62:6, 67:20, 74:2, 78:6, 95:7, 95:11, 98:5, 99:3, 102:15, 107:20, 128:7, 161:21, 162:3, 162:18, 189:19, 207:14, 226:9

Q

qualify 135:15
query 141:9, 141:13, 141:20
questioning 36:5, 255:18
questions 11:11, 36:2, 64:11, 94:20, 98:21, 102:21, 135:18, 197:4, 197:9, 197:10, 197:15, 197:17, 198:5, 198:7, 198:8, 198:11, 198:13, 294:17, 294:18
quick 291:9
quiet 91:17
quite 175:16
quote 78:7, 111:2

R

race 140:7, 140:21
raise 197:12, 197:14
raising 206:19
random 76:2, 98:2
range 57:16
ranger 52:7, 52:8, 52:12, 79:2
rank 105:13
ranked 105:16
rate 104:12, 104:20
rated 53:8
rather 50:3, 64:16, 136:13
rating 104:11
rationale 245:13
raw 73:12, 273:13, 274:5, 274:8, 274:20
reaction 270:5
read 13:4, 17:14, 18:5, 19:21, 27:7, 41:16, 45:22, 46:3, 46:6, 47:3, 48:3, 53:6, 58:4, 65:13, 67:1, 88:6, 92:11, 97:17, 99:7, 102:5, 108:9, 110:5, 112:10, 114:9, 115:5, 119:18, 120:2, 133:11, 139:6, 144:13, 145:21, 146:3, 146:11, 146:22, 148:12, 148:19, 149:16, 158:19, 158:22, 159:21, 160:1, 160:6, 165:2, 165:9, 165:13, 166:12, 167:21, 169:12, 172:5, 193:13, 205:18, 207:4, 207:6, 207:14, 224:15, 224:17, 224:18, 225:1, 229:1, 235:22,

236:3, 236:5, 249:10, 261:2, 263:19, 265:2, 266:21, 282:13, 292:16, 295:3
reading
26:19, 40:22, 43:10, 43:20, 64:15, 71:18, 75:3, 77:7, 90:2, 110:16, 112:5, 116:6, 118:14, 119:2, 121:6, 132:20, 132:21, 147:7, 161:22, 165:19, 166:17, 171:16, 210:19, 216:7, 220:3, 222:12, 223:10, 241:13, 242:19, 243:5, 243:17, 243:20, 261:22, 269:3, 270:2
reads
168:5
real
61:11, 65:10, 65:11, 65:15, 65:17, 68:19, 69:17, 79:14
realistic
188:3
reality
166:22
realize
257:12
really
32:14, 32:16, 32:18, 39:17, 39:20, 56:8, 64:11, 73:18, 74:22, 86:7, 86:22, 107:12, 113:10, 130:18, 132:7, 134:20, 135:10, 137:4, 138:21, 139:1, 139:2, 147:4, 150:10, 154:4, 155:14, 166:2, 166:8, 174:6, 174:15, 179:5, 181:2, 181:3, 189:15, 195:10, 196:12, 208:13, 209:18, 210:9, 211:18, 213:16, 213:19, 219:4, 225:8, 237:4, 238:15, 255:6, 255:11, 258:17, 258:22, 277:16, 285:2, 286:8, 288:6, 289:2, 292:11, 293:6
realsecure
53:10, 66:16, 78:14, 82:12, 83:18, 101:16, 247:7, 247:12, 250:12, 252:7, 253:12, 254:10, 255:1, 255:21, 255:22, 256:5, 258:10, 273:15, 273:21
realsecure's
256:20
realtime
96:1, 129:3, 131:4, 132:14
reason
42:6, 122:16, 185:9, 194:20, 196:19, 200:13
reasonable
179:16
reasons
274:6
recall
11:14, 11:20, 12:2, 12:6, 12:7, 18:15, 30:8, 30:16, 31:6, 31:17, 33:17, 52:13, 52:21, 57:15, 122:14, 123:15, 124:3, 124:8, 124:16, 125:22, 126:20, 128:3, 128:4, 246:20, 247:9, 247:11
receive
82:21, 264:1, 281:17
received
45:17
receiver
15:22, 16:15
receiving
15:22, 16:16, 46:10, 103:6, 104:15
recess
51:5, 106:1, 150:21, 211:22, 259:4, 291:11
recite
289:5
recited
221:1, 221:10
recites
239:2
recognitions
286:5
recognize
5:11, 266:22
recognized
266:17
record
53:6, 58:4, 65:13, 70:22, 99:3, 139:21, 168:16, 207:15, 261:2, 266:21, 296:9
recorded
53:7
recorder
53:10
redefine
45:7
refer
6:15, 13:15, 18:12, 109:19, 127:15, 194:11, 234:22, 251:3, 292:2, 292:3
reference
37:14, 37:18, 45:19, 124:20, 124:21, 125:1, 216:22, 217:3, 217:9, 240:2, 247:13, 248:17, 274:14, 275:15, 287:14, 288:1, 288:2
referenced
222:12, 274:14
references
17:6, 29:4, 29:6, 29:19, 30:10, 124:17, 245:15, 245:18, 246:1, 246:7, 246:13, 246:16, 246:19, 246:20, 247:1, 248:19, 249:3, 250:15, 250:16, 250:18, 283:5, 283:15
referred
67:16, 118:3
referring
52:6, 103:21, 154:3, 262:9, 272:14, 272:21, 275:11, 276:9, 278:2, 292:4
refers
106:8
refined
46:7
reflected
171:6
reflecting
16:1
reflection
99:8

refresh
58:20, 226:22, 235:22, 246:13, 263:11
refreshed
29:17
regard
67:7
regarding
92:3, 266:22
register
124:18
registered
126:5
related
66:15, 77:15, 99:16, 109:7, 178:1, 252:5, 274:14, 284:15, 296:18
relates
260:5
relating
29:2
relationship
153:11
relative
101:1, 101:12
relatively
57:2, 160:7, 276:4, 276:6
relatives
100:22
release
138:20, 138:22, 140:2, 143:16, 149:1, 150:6, 155:3
released
152:20, 165:1, 167:10
relevant
73:6, 183:3, 184:11
reliable
164:21
relies
66:2, 167:6
rely
63:4, 64:17, 87:19, 90:17, 120:8, 134:3, 134:4, 134:22, 147:11, 148:3, 148:4, 153:20, 155:8, 158:21, 271:14
relying
92:11, 92:21, 229:16, 270:22
remain
91:17, 116:12
remained
275:19
remaining
42:15, 44:8, 44:10, 220:15, 224:5, 233:1, 268:21
remains
142:12, 194:15, 203:15, 225:13
remember
29:13, 52:2, 52:11, 56:22, 137:19, 157:3, 181:15, 181:16, 181:22, 182:2, 182:13, 187:15, 197:18, 273:4, 276:13, 282:9, 288:2
remote
6:22, 7:5, 53:15, 53:17, 54:12, 54:18, 54:20, 55:4, 55:10, 55:13, 56:2, 56:11, 56:14, 57:4, 57:11, 57:17, 59:19, 60:2, 60:19, 60:20, 65:17, 67:17, 67:19, 67:21, 68:11, 68:14, 68:15, 68:16, 68:20, 69:18, 69:21, 70:5, 72:13, 74:5, 74:6, 74:11, 74:17, 75:7, 76:1, 76:2, 76:5, 76:6, 76:22, 77:13, 78:2, 79:15, 83:19, 85:19, 86:16, 89:5, 93:17, 93:18, 95:15, 96:22, 98:7, 98:14, 99:6, 99:18, 100:7, 100:13, 100:15, 100:16, 101:5, 101:11, 101:17, 102:1, 103:6, 104:6, 104:16, 105:4, 105:12, 105:16, 127:17, 247:12, 252:21, 253:14, 254:2, 254:15, 254:19, 255:3, 255:5, 255:9, 255:21, 256:6, 273:21
remotely
56:6, 56:9, 56:10, 59:7, 59:15, 60:14, 253:8
render
133:13
rendering
11:17
repeat
18:1, 30:3, 30:22, 33:2, 51:10, 60:1, 118:19, 146:8, 161:6, 171:21, 175:12, 178:11, 214:3, 219:9, 227:1, 249:2, 263:15, 267:16, 272:9
rephrase
185:19, 185:21
report
11:12, 17:18, 19:10, 19:18, 20:8, 21:13, 21:14, 23:6, 23:15, 23:20, 28:5, 29:5, 29:6, 29:20, 30:16, 30:18, 32:5, 32:9, 34:4, 34:9, 36:1, 36:3, 52:12, 65:18, 67:3, 67:6, 68:5, 69:1, 69:2, 69:3, 69:6, 69:10, 74:3, 77:9, 79:16, 80:5, 83:20, 84:1, 85:21, 87:13, 92:16, 94:16, 95:9, 95:18, 96:14, 97:5, 97:12, 98:5, 98:6, 99:14, 100:1, 101:17, 104:10, 105:4, 108:21, 109:3, 125:6, 171:13, 171:15, 179:4, 179:17, 193:7, 195:15, 229:9, 229:11, 230:7, 230:9, 235:1, 239:7, 239:13, 239:14, 256:7, 263:3, 266:5, 269:3, 273:22, 274:16, 277:21, 282:14, 283:4, 283:16, 283:20
reported
1:22, 83:11

reporter
96:11, 143:12
reporter-notary
296:1
reporting
77:7
reports
68:17, 68:18, 69:5, 69:16, 73:7, 89:5, 101:16, 102:14, 103:17, 131:22, 235:19, 273:12, 274:3
represented
9:15, 35:10, 107:4, 199:15, 201:7, 296:11
reputation
184:17
require
10:6, 10:17, 13:5, 14:6, 16:5, 16:12, 16:20, 175:11, 175:14, 176:1, 176:16, 243:22, 253:18, 277:5, 278:13, 279:19
required
15:18, 222:2, 227:9, 240:13, 241:22, 261:19, 263:9, 263:18, 267:10, 267:20, 277:1, 278:5, 293:15
requirement
221:21
requirements
132:14, 244:5, 265:16
requires
9:1, 45:14, 122:18, 150:9, 170:17, 199:9, 266:9
research
67:10, 67:13, 70:16, 84:19, 85:22, 86:17, 87:22, 128:4, 129:18, 131:19, 157:5, 257:2, 258:18
reserved
172:19
resided
267:1
residues
59:12, 179:12
resolve
239:21
resource
128:7
respect
21:8, 54:4, 67:21, 68:16, 95:22, 96:5, 100:15, 102:1, 115:3, 157:21, 166:10, 250:7, 255:13, 255:16, 281:6, 293:21
respond
58:12, 62:16, 63:12, 63:15, 65:5, 79:7, 79:22, 80:11, 80:16, 81:3, 81:9, 83:17, 273:9, 278:20
response
58:1, 58:5, 58:13, 63:16, 79:19, 247:19, 275:7, 276:19, 278:17, 278:22, 279:2, 279:13, 279:18, 280:2, 280:10, 281:1, 281:18, 282:5, 282:7, 282:16, 282:19, 282:22, 283:11, 283:22, 285:2
rest
153:14, 154:8, 208:6, 208:9
restart
47:22, 50:3, 50:4, 50:18
restore
132:16
restriction
190:15
result
142:8
results
38:13
resume
152:21, 167:11
retain
41:13, 44:1, 203:7, 204:1, 205:17, 210:18, 285:22, 287:6
retaining
205:20
retrieve
141:13, 141:20, 142:22, 144:19
review
24:11, 38:3, 46:2, 55:9, 66:13, 179:2, 225:2, 235:3, 236:4, 239:10, 263:13, 268:1
rhetorical
64:11
right-hand
8:10, 8:15, 8:16, 13:19, 43:13
risk
179:22, 180:3, 180:7, 181:20, 183:1, 187:19
rmr
1:22, 2:11, 296:2, 297:10
romanette
226:12
room
101:11
rose
2:5, 3:13, 296:15
route
178:2, 178:5
rule
100:11, 159:8, 159:12, 160:17, 161:8, 162:10, 162:15, 162:20, 168:7, 169:6, 169:15, 169:16, 172:7, 172:9, 172:11, 172:12, 172:15, 172:16, 172:20, 172:21, 173:2, 173:10, 211:9, 216:19
rule-matching
216:9, 216:10
rules
38:11, 38:19, 41:8, 43:21, 73:9, 159:2, 159:22, 161:12, 161:18, 162:1, 162:4, 162:21, 163:12, 163:14, 165:13, 166:13, 169:14, 169:21, 169:22, 171:7, 171:19, 171:22, 172:1, 190:2, 190:9, 191:1, 213:7, 214:21
run
55:16, 141:12, 141:19, 141:20, 160:14, 254:22
running
128:5, 134:22, 155:18, 171:7

S

s
43:19, 44:20, 48:2, 50:22, 51:8, 51:12,

56:18, 56:21, 59:2, 69:19, 126:16, 128:1, 128:10, 130:2, 130:14, 132:3, 133:7, 134:6, 151:6, 181:9, 181:10, 182:13, 182:14
s----------
4:10
s-o-c-r-a-t-e-s
239:21
sa
55:12
safe
46:15, 65:15
same
14:18, 30:7, 30:22, 31:4, 43:2, 60:5, 69:22, 73:4, 73:5, 77:5, 82:6, 91:6, 97:9, 100:19, 101:2, 101:3, 101:7, 101:9, 101:10, 113:16, 121:2, 135:16, 137:8, 139:8, 139:12, 141:6, 143:1, 145:13, 158:18, 158:21, 159:4, 162:11, 162:16, 163:1, 163:12, 166:15, 168:3, 170:4, 170:9, 173:1, 185:2, 185:9, 186:3, 193:15, 194:10, 195:11, 196:12, 196:20, 199:9, 210:20, 213:2, 258:2, 258:3, 277:22, 280:5, 282:15, 295:4
satisfies
125:3
saw
53:3
saying
20:14, 21:7, 23:19, 24:20, 37:5, 43:18, 62:1, 63:2, 63:10, 76:14, 83:15, 95:3, 103:1, 119:13, 136:1, 144:9, 154:1, 155:7, 170:2, 170:3, 170:16, 170:22, 174:10, 182:9, 183:2, 187:16, 187:19, 203:20, 204:2, 204:7, 211:17, 215:9, 221:20, 222:21, 223:5, 224:19, 225:3, 225:5, 225:10, 229:9, 237:10, 238:21, 262:20, 278:15, 279:15, 293:1
says
7:3, 9:4, 9:12, 9:18, 12:21, 13:11, 14:11, 16:15, 22:9, 23:6, 31:21, 34:11, 35:2, 36:19, 37:10, 38:6, 42:1, 48:7, 53:1, 58:1, 60:6, 62:4, 64:16, 65:3, 65:11, 66:1, 68:5, 68:19, 69:5, 71:20, 72:4, 79:14, 80:7, 80:9, 80:18, 83:19, 84:1, 84:10, 88:13, 90:21, 91:3, 103:5, 103:20, 104:18, 108:3, 115:12, 117:6, 119:19, 128:12, 128:15, 139:15, 157:15, 157:22, 159:13, 165:15, 175:3, 193:13, 200:16, 201:8, 201:17, 201:18, 201:21, 202:2, 202:8, 202:12, 203:10, 205:21, 215:22, 219:7, 223:8, 227:17, 231:9, 240:4, 240:8, 251:6, 263:20, 264:10, 266:17, 271:22, 273:10, 292:4, 293:18
scale
170:20
scanning
65:14
scenario
136:14, 137:7, 146:17, 152:1, 154:13, 160:15, 163:21
scenarios
133:2
schneier
19:13, 19:19, 20:6, 20:12, 21:22, 22:8, 23:1, 23:22, 26:16, 29:14, 30:19, 31:14, 36:18, 39:8, 44:12, 59:17, 60:15, 61:2, 69:22, 97:17, 108:11, 123:20, 220:4, 224:16, 239:8, 239:17, 240:2, 240:19, 268:6, 280:19, 284:8, 286:18, 288:3, 288:8, 288:22, 289:22, 290:17
schneier's
59:5, 61:5, 239:18
school
184:9
science
132:18, 138:4, 140:18, 141:1, 161:19, 162:22
sciences
275:22
screen
81:21, 82:1
screw
129:10, 129:11
script
129:13
scripts
63:20
sea
42:15
seal
297:3
search
48:10
second
10:5, 10:7, 10:12, 10:18, 11:2, 11:7, 11:14, 12:4, 46:4, 52:2, 60:10, 70:14, 71:19, 72:10, 79:12, 99:4, 145:17, 146:3, 146:11, 148:13, 149:16, 186:5, 189:18, 196:14, 234:15, 235:15, 250:14, 258:6, 258:10
secondly
252:15
section
66:1, 66:13,

227:8, 228:6, 229:1, 260:1, 261:8, 261:13, 261:18, 262:3, 262:12, 262:14, 262:19, 262:21, 263:8, 263:17, 264:14, 264:15, 264:22, 265:19, 266:3, 285:15
sections
264:14
secure
8:11, 38:14, 46:8, 59:3, 61:11, 63:11, 65:10, 65:11, 65:15, 65:17, 68:19, 69:17, 70:1, 74:8, 79:14, 97:1, 97:11, 98:6, 111:15, 118:7, 182:3, 186:13, 186:16, 186:17, 189:6, 238:2, 241:11, 241:15, 242:9, 244:16, 244:17, 244:20, 257:19, 264:1, 265:8
secured
242:20
security-related
9:14, 12:11, 13:6, 14:7, 35:10, 77:11, 98:2, 103:21, 104:5, 107:4, 176:14, 176:19, 176:22, 177:1, 177:4, 177:8, 177:10, 177:19, 178:9, 178:13, 178:15, 178:17, 181:1, 185:4, 185:13, 186:2, 187:1, 192:12, 193:3, 193:6, 194:3, 199:14, 201:7, 214:17, 272:17, 274:11, 284:14
seeing
10:4, 122:14, 124:8, 128:3
seems
58:15, 166:13, 166:18, 230:1, 245:14, 251:7
seen
6:18, 28:2, 28:20, 52:19, 52:20, 123:1, 126:5, 283:1
select
112:12, 112:22, 114:21, 116:10, 118:5, 118:8, 141:11, 142:6, 189:3
selected
35:14, 40:19, 107:8, 115:7, 115:18, 117:15, 119:21, 120:10, 120:19, 194:8, 199:19, 199:22, 200:1, 200:2, 202:3, 202:10
selecting
121:11, 142:7
selects
108:15, 109:17
self-related
177:3
send
40:4, 40:6, 40:21, 42:8, 42:9, 47:15, 59:12, 68:17, 69:5, 69:12, 69:15, 73:5, 73:7, 73:20, 74:1, 74:4, 74:16, 75:15, 75:18, 76:1, 76:7, 76:19, 78:22, 83:20, 93:7, 98:2, 99:7, 99:12, 99:13, 99:15, 99:16, 99:18, 151:16, 160:2, 177:12, 183:14, 242:21, 274:3, 274:17
sender
76:2, 76:22, 78:2
sending
39:19, 67:3, 72:22, 75:20, 77:6, 79:4, 79:17, 82:2, 99:22
sends
38:13, 43:9, 84:1
sense
50:20, 50:21, 67:20, 74:6, 75:21, 81:2, 100:17, 106:13, 110:6, 151:17, 173:6, 188:5, 209:8, 222:18, 231:12, 232:9, 233:1
sensical
223:17
sensing
65:17, 67:17, 67:19, 68:11, 68:14, 68:20, 72:13, 74:11, 75:7, 77:13, 79:15, 83:19, 99:6, 102:1, 256:6, 273:21
sensor
75:14, 77:4, 110:1, 110:15, 159:2, 194:13, 194:22, 195:5, 220:12
sensors
109:22, 110:10, 110:12, 253:9, 253:22
sent
37:3, 42:4, 73:13, 73:14, 74:10, 75:6, 75:8, 75:10, 75:22, 77:13, 77:14, 78:17, 79:8, 80:5, 81:12, 83:14, 94:16, 95:9, 95:14, 95:18, 96:14, 97:5, 97:10, 98:6, 109:4, 109:8, 115:9, 194:18, 270:14
sentence
19:12, 22:2, 22:4, 25:15, 26:20, 31:13, 31:19, 31:21, 34:11, 35:6, 37:1, 37:10, 42:1, 45:4, 45:11, 45:12, 46:7, 46:11, 46:20, 51:10, 54:11, 54:19, 55:5, 55:10, 55:18, 57:4, 60:10, 70:14, 71:19, 72:4, 72:10, 79:12, 79:13, 86:19, 109:10, 111:2, 180:4, 180:8, 205:11, 207:6, 224:12, 227:17, 235:16, 245:11, 245:22, 246:4, 250:14, 251:6, 254:18, 259:9,

259:15, 260:20, 260:22, 266:17, 268:4, 269:22, 270:3, 270:11, 270:16, 271:22
sentries 34:11, 35:2, 268:10, 269:15
sentry 8:13, 8:15, 37:1, 37:11, 38:5, 38:10, 38:17, 39:5, 40:14, 40:22, 41:7, 41:16, 41:19, 42:2, 43:7, 43:13, 43:15, 158:1, 267:3, 270:12, 271:6
separate 138:7, 156:8, 214:22, 215:8, 216:13, 216:19, 225:7
server 127:10, 127:11, 127:12, 127:13, 127:14, 127:16, 128:1, 131:12, 292:6
servers 46:14
service 17:21, 18:3, 46:18, 46:19, 47:15, 50:16, 51:8, 51:12, 51:17, 52:3, 52:8, 56:2, 57:12, 58:6, 58:21, 60:2, 61:13, 62:5, 66:6, 66:16, 66:18, 69:18, 75:1, 76:5, 76:6, 78:18, 78:19, 79:20, 98:7, 98:15, 253:18, 272:22, 273:15, 289:20
services 47:22, 53:15, 53:18, 54:13, 54:20, 55:5, 55:11, 56:15, 56:18, 57:5, 57:17, 59:19, 70:5, 73:19, 93:17, 96:22, 98:14, 252:21, 253:6, 253:16, 254:16, 254:20, 255:3, 255:5, 255:22, 275:19, 276:3, 286:11
servicing 111:19
session 53:11, 67:2
set 38:11, 132:13, 178:8, 277:16, 279:16, 290:19, 296:6, 297:2
sets 41:8, 279:13
setting 125:22
seven 58:9
several 23:13
severity 103:13, 103:20, 104:19, 105:2, 105:5, 105:7, 105:13, 105:18
shall 191:2, 243:4
share 246:21
sheer 272:4
sheet 295:7
shocked 242:7
short-handed 18:15
shortcut 264:18
shorthand 296:1
should 22:2, 22:3, 42:10, 105:21, 150:18, 177:4, 182:22, 183:18, 184:19, 190:21, 213:7, 213:11, 216:3, 216:4, 216:12, 219:2, 225:6, 225:9, 228:2, 250:19, 262:16, 264:4, 265:5, 269:2, 294:10
shouldn't 75:18
show 25:10, 26:8, 27:2, 30:12, 31:8, 31:22, 37:22, 45:12, 129:21, 246:1, 250:16, 250:18, 267:7, 285:18, 287:11, 289:12
showing 225:18, 225:20, 226:2, 226:21, 229:22, 287:2
shown 35:7, 37:5, 37:14, 229:3, 256:1, 267:17
shows 48:20
shut 49:19, 50:2, 50:4, 50:18, 145:8, 147:12, 148:6, 152:19, 153:22, 155:9, 164:22
shutting 47:14, 50:13, 141:21, 142:3, 142:5, 142:17, 142:18, 143:1, 143:14, 144:6, 144:20, 145:11
sic 223:17
side 8:7, 8:9, 8:10, 8:14, 8:15, 8:16, 13:16, 13:17, 13:18, 13:19, 43:12, 43:13, 47:16, 47:17, 67:20, 67:21, 68:15, 68:21, 78:15, 85:21, 99:18, 101:10, 182:8, 240:22, 242:8, 242:22, 254:1
sign 75:2
signature 5:17, 295:10
signature-p1kal 297:8
signatures 66:3, 66:9, 66:20, 70:13, 72:6, 84:12, 84:13, 86:4, 86:21, 93:21
signed 5:19, 295:7
similar 47:12, 72:17, 142:17, 214:19
simple 145:14, 148:14, 152:4, 167:21, 168:18
simply 206:18, 230:17

since
11:3, 25:6, 28:12, 29:13, 48:15, 82:18, 126:15
single
20:15, 22:6, 22:10, 22:12, 31:21, 32:11, 55:12, 133:6, 140:11, 148:10, 150:4, 160:9, 162:13, 162:16, 163:2, 163:10, 165:11, 173:7, 173:17, 173:18, 174:6, 174:11, 174:18, 209:9, 209:10, 290:9
sir
95:22, 141:18, 206:6
sit
88:16, 129:22, 130:12, 131:9, 136:15, 149:13, 168:22, 181:17, 257:14
site
93:18, 177:18, 177:19, 178:17, 182:19, 182:22, 183:17, 183:18, 184:3, 184:8, 186:1, 186:5, 186:7, 187:18, 190:20, 191:7, 191:22, 192:6, 193:3
sites
181:11, 181:18, 181:19, 182:1, 182:2, 182:3, 182:13, 183:16, 184:15, 185:10, 185:12, 187:9, 188:13, 191:21
sitting
84:4, 133:10
situation
7:10, 130:19, 132:8, 133:7, 147:4, 147:6, 147:16, 150:1, 150:8, 150:11, 153:13, 154:5, 157:10, 157:13, 164:2, 164:16, 164:17, 168:11
situations
133:2, 134:21
six
194:12
skill
38:21, 40:1, 42:11, 64:2, 64:15, 66:17, 115:21, 117:9, 156:19, 175:20, 248:21, 249:5, 257:11, 257:16, 290:16, 291:2
skills
62:12, 62:13
small
40:20
smaller
47:18, 276:7
smirk
35:21
so-called
67:19, 140:7, 183:15, 285:19, 287:3, 289:12
soc
8:10, 37:3, 39:20, 40:5, 40:21, 41:18, 42:4, 42:8, 43:9, 43:14, 81:17, 82:5, 83:10, 83:11, 83:14, 95:15, 97:1, 97:22, 182:3, 187:6, 240:22, 241:15, 242:9, 270:14
socrates
8:19, 37:3, 41:18, 42:4, 43:14, 45:6, 109:5, 239:21, 270:15
software
129:1, 138:11, 157:22, 159:20
solely
92:10
solution
53:9
solve
159:10
some
8:13, 13:19, 15:3, 15:13, 29:4, 40:11, 42:10, 44:8, 57:2, 57:7, 72:17, 73:19, 78:15, 87:15, 92:3, 95:16, 97:20, 98:10, 99:14, 104:11, 109:5, 112:7, 146:15, 150:8, 150:9, 157:9, 158:21, 159:7, 169:6, 170:18, 179:18, 180:14, 182:5, 186:7, 191:1, 211:11, 214:9, 231:20, 234:2, 234:20, 237:16, 238:6, 254:5, 254:7, 256:12, 287:15
somebody
81:22, 150:10
somehow
48:20, 98:5
someone
144:5
something
11:9, 40:19, 51:22, 62:6, 74:6, 74:17, 75:22, 76:22, 93:4, 112:3, 112:10, 113:7, 113:21, 117:21, 119:3, 122:3, 122:20, 122:21, 124:11, 125:3, 125:13, 126:5, 126:8, 142:8, 142:17, 147:20, 149:9, 150:7, 156:20, 157:8, 160:2, 170:14, 178:8, 186:11, 187:21, 191:8, 198:4, 214:4, 231:17, 233:9, 233:15, 237:21, 249:15, 270:8
sometimes
18:12, 179:21, 180:2, 187:5, 235:20, 257:22
somewhere
97:6, 102:3
soon
29:13
sophisticated
58:14
sorry
10:14, 14:19, 34:16, 38:13, 39:2, 54:17, 62:8, 73:10, 77:19, 77:20, 93:5, 108:10, 117:13, 124:6, 151:13, 171:22, 193:8, 202:19, 210:22, 219:9, 227:1, 235:8, 235:19, 244:3, 250:9, 259:10
sort
74:10, 105:2, 105:10, 123:5, 125:22, 159:8,

163:7, 178:8, 212:18, 231:20, 237:12, 256:12, 293:13
sounds 36:13
source 71:21, 86:3
sourced 160:10
sources 186:20
space 183:7, 232:5, 275:2
spam 183:14
spans 285:15
speakers 206:7, 206:13
spec 114:15, 148:19, 241:19, 293:8
specific 12:14, 22:20, 26:5, 26:6, 26:7, 26:9, 33:17, 58:9, 71:5, 75:3, 82:7, 93:2, 93:4, 93:5, 93:6, 93:13, 94:19, 96:20, 98:10, 98:15, 98:22, 107:21, 107:22, 108:20, 108:22, 109:1, 122:17, 136:13, 148:9, 157:9, 171:14, 172:15, 178:16, 179:18, 181:22, 190:1, 192:2, 213:17, 215:3, 216:14, 239:8, 243:22, 244:5, 262:12, 288:13, 290:10
specifically 30:17, 31:16, 79:17, 80:5, 113:9, 113:18, 114:17, 126:1, 126:20, 184:7, 204:16, 216:7, 227:22, 272:21, 286:6
specification 114:16, 239:18
specified 277:5, 278:13
specifies 281:2
specify 22:1, 189:13, 222:6, 240:12, 241:21, 277:1, 278:5
spend 168:10, 169:11
spending 150:2
spot 102:18, 102:22
spyware 181:13
sql 127:10, 127:11, 127:13, 128:1, 131:12, 137:13, 141:5, 141:10
square 2:6, 3:14, 296:15
sri 233:20
ss 43:1
ssl 241:12
staff 58:16
staffed 58:9
staffing 58:6, 60:10, 63:3, 64:16
stand 175:8, 193:19, 197:20, 276:21
standard 243:7
stands 266:6, 282:15
start 61:12, 190:3, 193:22, 195:17, 198:2, 200:8, 217:18, 218:10, 218:15, 218:16, 219:7, 219:12, 219:13, 219:19, 219:20, 250:17, 291:20, 294:3
start" 219:7
started 70:2, 98:20, 198:3
starting 34:4, 52:1, 57:2, 109:10, 110:13, 110:14, 111:3, 112:11, 114:9, 118:4, 158:14, 165:1, 179:4, 188:21, 241:8, 293:18
starts 54:12, 217:12, 228:22, 260:20, 294:13
state 2:12, 19:4, 61:18, 245:19, 246:8, 247:15, 248:4, 248:7, 248:16, 249:18, 249:21, 250:6, 250:13, 255:14, 255:15, 296:3
state-of-the-art 252:17
stated 21:14, 22:17, 23:15, 23:20, 80:6, 120:1, 121:9
statement 22:21, 24:4, 55:1, 61:15, 107:14, 107:16, 107:18, 120:8, 137:1, 175:8, 192:15, 215:16, 215:17, 215:21, 220:9, 259:22, 264:13, 265:20, 276:21
states 1:1, 199:20
static 47:7, 47:9
statically 47:21, 127:4
stating 17:17
station 65:18, 67:19
stations 67:17, 68:12, 68:20, 79:15, 83:19, 101:17, 256:6, 273:22
status 9:2, 9:4, 9:13, 9:15, 35:9, 35:10, 39:9, 107:3, 107:4, 109:22, 110:15, 176:13, 194:2, 194:4, 194:14, 199:15, 200:18, 200:21, 201:5, 201:7, 201:15, 201:19, 201:22, 202:4, 202:13, 203:4, 203:10, 203:12, 203:14, 203:16, 203:21, 204:8, 204:10, 204:12, 205:14, 205:21, 205:22,

206:5, 207:20, 207:21, 208:4, 208:15, 208:20, 208:21, 209:2, 209:13, 209:20, 210:7, 210:12, 210:16, 211:2, 212:7, 212:12, 212:14, 212:15, 213:8, 213:9, 213:16, 214:15, 215:14, 215:22, 216:2, 216:11, 226:14, 227:18, 234:15, 234:17, 234:18, 235:7, 236:6, 236:7, 236:9, 236:10, 236:12, 237:2, 237:5, 237:13, 237:14, 237:15, 237:20, 237:21, 238:1, 238:4, 238:7, 238:11, 238:18, 269:12, 284:13
stay
141:1
steal
182:16
step
40:14, 163:4, 219:6, 259:18, 264:5, 265:4, 265:13, 265:14, 266:8, 266:11, 291:19, 292:10, 292:11, 293:7, 293:9, 293:14, 293:15, 293:19
steps
225:18, 226:2
sterne
3:5
still
20:9, 25:7, 40:11, 70:3, 128:2, 128:11, 133:9, 134:19, 136:6, 143:22, 153:16, 160:17, 161:9, 163:19, 171:7, 200:15, 205:21, 209:12, 212:5, 263:2, 276:4, 276:6, 281:11
stop
190:15
stopped
152:19, 167:9
storage
127:1, 127:3, 128:21, 129:4, 129:6, 129:18, 130:20, 132:10, 132:11, 135:3, 137:11, 145:3
stored
171:20, 172:2
story
83:13
straight
79:8, 138:10
straightforward
160:8
strange
223:21
stream
195:18, 195:20, 219:16, 292:9, 292:13, 292:15, 292:20, 293:10
strength
58:8, 60:12, 63:4, 64:17
strict
138:3
student
47:12, 48:18, 140:18
students
157:4, 184:18
studying
150:3
stuff
29:19, 29:21, 43:9, 77:11, 123:22, 124:9, 234:12, 256:13
submitted
54:4, 122:12, 204:18
subsection
226:12, 227:3, 227:15, 228:22, 285:10
subsystem
9:8, 9:12, 9:21, 12:9, 35:8, 106:9, 108:13, 108:14, 108:19, 109:16, 115:7, 115:9, 115:19, 117:14, 117:16, 119:20, 119:22, 176:12, 194:2, 199:13, 200:17, 200:20, 201:1, 201:18, 203:4, 203:21, 204:3, 204:11, 204:12, 205:14, 207:20, 208:3, 208:8, 208:9, 208:15, 209:1, 209:2, 209:13, 209:14, 209:17, 210:7, 210:11, 210:21, 211:1, 211:6, 212:5, 212:7, 212:18, 213:15, 214:12, 214:14, 215:14, 216:10, 220:17, 221:5, 221:16, 222:13, 226:14
success
285:11, 285:20, 287:4, 288:16, 289:13
sufficient
31:20, 32:8, 32:10, 32:12, 158:6, 242:5
suggest
66:16
suggesting
63:5, 64:19
suggestion
235:4
suggests
259:16
suit
65:15
super
129:5, 129:19, 131:20, 133:14, 137:11, 155:18, 156:1, 156:21, 157:2, 157:7, 157:21, 158:7
super-challenging
159:11
superset
177:2
supplement
125:21
support
54:4, 196:14, 259:22, 261:7, 264:13
supporting
25:20, 86:19
supports
65:17, 68:19, 79:15, 256:6, 273:21
suppose
192:3
supposed
159:16
supposedly
262:6
sure
40:11, 40:15, 42:7, 42:20, 42:22, 43:4, 44:17, 44:18, 44:21, 44:22, 51:19, 52:20, 69:16, 72:3, 77:13, 127:9,

131:3, 166:20, 187:3, 190:21, 192:20, 203:19, 232:20, 247:3
surrounding
288:22
susceptible
181:12
suspected
97:21
sworn
5:4, 296:6
sync
129:8, 135:5
synchronization
129:5, 135:8, 160:13
synchronize
128:4, 129:16, 137:9
synchronized
131:4
synthesizing
245:2, 248:1, 277:12, 282:1
systems
8:8, 56:11, 99:6, 132:17, 214:20, 215:7, 240:8, 272:2, 272:19, 275:22, 276:3, 282:12, 284:21

T

table
135:6, 135:7, 137:14, 137:18, 138:15, 138:16, 138:17, 138:18, 138:19, 142:5, 142:17, 142:18, 142:21, 142:22, 143:1, 143:8, 143:13, 144:10, 144:13, 144:14, 144:17, 144:19, 145:7, 145:9, 145:12, 145:17, 145:18, 146:3, 146:4, 146:11, 146:12, 146:15, 146:16, 146:18, 146:22, 147:1, 147:10, 147:11, 147:19, 148:12, 148:13, 149:15, 149:16, 152:5, 152:8, 152:12, 152:15, 152:17, 153:2, 153:5, 153:10, 153:11, 153:14, 153:19, 153:21, 154:8, 154:15, 154:16, 155:5, 163:17, 164:19, 166:5, 167:4, 167:7, 260:5
tables
145:15, 145:22, 148:10, 152:3
take
24:6, 51:2, 76:2, 76:22, 81:1, 81:21, 81:22, 83:12, 90:20, 105:21, 149:5, 150:17, 165:2, 166:4, 195:4, 209:6, 210:1, 246:21, 255:18, 257:8, 258:8, 259:3, 263:10, 267:22, 285:5, 287:14, 291:9
taken
226:3, 293:20, 293:21, 294:9, 296:8
taking
91:16
talk
22:21, 26:5, 27:8, 29:14, 30:18, 31:7, 32:12, 34:4, 36:17, 39:14, 41:19, 42:5, 44:12, 44:20, 47:13, 51:22, 52:13, 55:20, 56:4, 56:7, 56:14, 57:4, 57:17, 59:8, 59:13, 67:4, 67:8, 67:13, 68:3, 68:7, 71:1, 77:3, 79:4, 79:16, 84:8, 85:18, 85:20, 89:4, 98:13, 98:15, 98:16, 98:19, 99:2, 99:9, 121:3, 122:14, 124:2, 125:6, 126:1, 135:10, 140:21, 168:20, 173:7, 179:8, 183:13, 188:22, 191:20, 191:22, 192:4, 192:5, 192:22, 194:12, 206:3, 207:3, 210:15, 228:15, 228:16, 233:6, 233:13, 234:15, 235:7, 239:6, 241:11, 242:20, 255:7, 257:4, 257:6, 268:8, 268:9, 268:10, 274:15, 275:15, 275:16, 278:3, 278:4, 278:16, 280:1, 282:3, 286:4
talked
11:13, 158:15, 163:21, 167:12, 231:8, 233:20, 253:1, 266:1
talking
6:16, 30:17, 43:5, 43:16, 56:1, 56:15, 60:15, 60:17, 63:22, 73:10, 73:22, 77:22, 98:7, 98:10, 107:12, 107:19, 113:5, 113:10, 114:11, 117:3, 117:5, 123:3, 123:4, 123:21, 124:1, 126:7, 126:22, 128:20, 130:22, 132:8, 132:9, 133:2, 133:16, 147:9, 147:14, 148:9, 151:3, 160:8, 165:4, 173:17, 174:7, 181:7, 196:17, 198:3, 206:10, 206:18, 207:2, 208:4, 212:4, 247:9, 247:21, 261:21, 261:22, 262:4, 262:8, 265:9, 269:11, 272:14, 274:8, 274:9, 274:18, 277:3, 289:19
task
174:17, 178:16
tasked
172:20
tasks
165:15
taught
117:19, 229:20
teach
50:7, 108:1, 115:14, 158:7, 190:12
teaches
37:15, 158:13, 177:15, 249:15,

260:21, 261:3, 264:10, 269:18, 269:22, 271:9, 271:10
teaching
38:1, 115:20, 116:13, 176:9, 181:5, 184:9, 192:8, 203:17, 243:18, 253:7, 253:11
team
58:7, 60:11, 63:3, 66:2, 70:12, 72:5, 72:14, 84:3, 84:10, 89:1, 89:2, 89:6, 89:10, 92:2, 256:15, 257:1, 257:4, 257:14, 258:15
teams
86:8, 87:3, 88:17, 89:19, 90:4, 90:11, 94:13, 256:20, 258:14
technical
29:22, 30:4, 190:14
technologies
28:16, 283:17
technology
29:12, 33:10, 34:5, 111:20, 131:2, 182:7, 233:22, 280:21, 286:21, 287:17
tell
32:10, 61:20, 62:4, 62:5, 62:13, 62:21, 63:17, 65:7, 71:2, 71:17, 75:16, 81:16, 90:21, 91:22, 94:4, 94:13, 133:14, 138:14, 159:19, 169:19, 169:22, 180:15, 180:16, 180:19, 183:8, 186:18, 189:14, 189:21, 190:8, 190:9, 190:10, 197:21, 198:18, 207:9, 208:5, 208:6, 208:11, 214:10, 238:7, 248:15, 290:4
telling
62:14, 63:1, 72:10, 72:11
tells
130:8, 138:21, 139:1, 139:2, 140:5, 140:7, 180:15, 195:10, 196:9, 208:8, 208:10, 216:11, 219:3, 237:14, 244:16, 253:13, 294:8
ten
234:6
term
10:3, 112:2, 112:7, 112:17, 173:8, 173:9, 234:21, 239:16
terms
39:18, 70:1, 101:11, 109:2, 109:6, 114:5, 114:6, 114:18, 162:6, 254:8, 286:14
terry
52:17
test
53:7
testified
5:5
testify
89:18
testifying
25:3, 25:4, 36:12, 83:2, 91:13
testimony
16:8, 16:22, 22:15, 26:12, 32:3, 32:20, 41:4, 41:9, 41:15, 43:18, 44:4, 49:3, 59:22, 63:8, 64:18, 65:2, 73:3, 78:6, 86:8, 86:12, 87:2, 87:7, 88:12, 88:16, 95:20, 100:21, 119:17, 120:4, 120:6, 129:22, 130:5, 130:11, 130:17, 136:15, 136:20, 149:13, 149:17, 149:20, 156:18, 157:1, 158:5, 170:16, 171:2, 178:20, 181:17, 183:6, 185:10, 185:15, 185:22, 192:14, 193:19, 202:7, 203:20, 204:4, 204:6, 204:15, 208:19, 210:10, 215:19, 230:19, 232:1, 238:10, 238:13, 250:1, 256:4, 269:21, 283:14, 288:19, 291:16, 294:7, 295:4, 295:5, 296:9
text
47:3, 66:15, 207:9
thank
103:2, 275:13, 291:14
themselves
244:2, 244:4
theoretically
272:1
thereof
45:16
theses
232:4
thesis
43:1, 125:8, 157:5, 184:18, 233:13, 233:17, 233:18
thing
40:7, 41:11, 43:2, 43:19, 50:8, 50:14, 50:19, 60:9, 60:13, 60:22, 62:12, 77:5, 83:13, 99:4, 105:10, 113:16, 122:20, 134:16, 135:16, 138:7, 139:20, 141:6, 145:2, 149:3, 149:6, 150:4, 161:2, 162:14, 162:22, 163:3, 163:10, 166:15, 170:8, 170:11, 170:12, 172:18, 172:21, 173:12, 174:20, 179:16, 186:6, 189:18, 192:21, 192:22, 195:3, 213:3, 213:22, 214:1, 214:7, 214:13, 219:12, 222:18, 223:17, 224:6, 232:21, 233:10, 233:11, 251:14, 258:5, 258:6, 258:10, 271:8, 281:9
things
9:1, 21:12,

40:7, 40:8, 40:9, 42:7, 42:8, 42:18, 43:4, 44:7, 45:20, 48:1, 60:17, 62:22, 67:16, 67:17, 74:2, 83:11, 90:16, 100:22, 106:22, 109:12, 110:2, 110:3, 110:19, 110:20, 111:4, 111:14, 116:10, 123:18, 125:19, 129:15, 135:2, 151:5, 163:1, 163:14, 165:11, 166:22, 170:10, 181:8, 181:22, 182:18, 183:10, 184:4, 184:5, 184:20, 185:1, 189:9, 189:10, 192:10, 194:15, 194:17, 201:1, 209:11, 223:11, 223:13, 224:1, 224:2, 224:3, 225:13, 232:7, 232:22, 234:14, 252:18, 258:14, 268:17, 268:19, 270:6, 270:9, 281:11
third
46:7, 169:12, 183:21, 186:6, 266:16
thought
68:10, 95:13, 202:17, 251:15
threat
45:8, 76:11, 185:13, 186:2, 190:3, 212:20
threats
34:13, 34:14, 35:4, 36:22, 38:9, 190:4, 190:9, 267:1, 268:12, 269:18, 272:3
three
34:21, 158:5, 163:5, 165:15
through
22:10, 28:9, 31:2, 179:5, 181:9, 181:10, 188:20, 195:8, 200:8, 200:9, 200:10, 208:7, 220:13, 226:18, 227:4, 227:7, 227:11, 243:19, 249:7, 254:3, 256:18, 263:12, 271:4, 274:1, 290:3, 292:18, 293:13, 294:3
throughout
29:19, 30:18, 34:3, 286:12
throw
42:12, 42:13, 44:6, 44:13, 110:2, 116:7, 194:14, 203:12, 222:15, 224:1, 224:2, 231:4, 268:16, 270:6
thursday
1:15, 296:16
ties
71:1, 71:6, 71:8
time
29:7, 40:12, 48:14, 49:6, 49:15, 64:3, 69:14, 70:3, 78:8, 92:4, 92:5, 94:11, 96:8, 111:11, 126:22, 131:11, 133:12, 139:8, 139:12, 141:16, 149:5, 150:16, 157:5, 162:11, 162:14, 162:16, 162:20, 163:2, 163:6, 163:8, 163:17, 163:18, 165:12, 165:16, 166:13, 166:18, 169:7, 170:4, 170:20, 172:19, 173:1, 173:13, 173:21, 174:1, 174:17, 174:20, 181:11, 183:8, 185:7, 198:7, 234:6, 258:11, 283:18, 290:17, 292:14, 294:19
times
2:6, 3:14, 23:13, 88:21, 90:15, 91:7, 121:17, 130:18, 134:9, 136:21, 200:8, 268:14, 274:2, 284:9, 286:15, 296:15
timestamp
57:1
title
53:3, 79:3
titled
52:16
today
86:8, 87:2, 88:16, 130:1, 149:14, 182:8, 183:13, 253:1, 268:14, 271:5, 276:5, 276:7
today's
274:2, 286:13
told
68:4, 68:10, 209:19
ton
42:9, 69:11, 75:14, 77:6, 129:18, 233:15
tool
184:9
tools
65:14
top
34:21, 84:2, 217:7, 294:13
topic
184:18
tos
241:12
total
101:20
touch
138:17, 139:22, 142:5, 142:19, 144:16, 156:4, 178:3, 178:12
touching
140:12, 156:10
toward
35:1
trademark
1:1
traditional
39:11, 43:7
traffic
39:9, 42:19, 44:6, 52:9, 62:18, 63:18, 68:7, 183:15, 203:6, 203:22, 204:13, 205:16, 206:1, 207:22, 208:5, 208:7, 208:20, 209:7, 209:14, 209:21, 210:3, 210:8, 210:12, 210:17, 211:4, 211:7, 211:11, 212:8, 213:10, 213:14, 213:17, 213:19, 214:6, 214:8, 215:4, 215:15, 216:1, 216:5,

216:7, 216:17, 272:17
trained
45:5, 239:19
transaction
128:22, 151:13
transactions
139:11
transcript
78:4
transcription
295:5
transmission
194:11, 195:11, 196:4, 196:6, 196:13, 196:21, 197:1, 200:6, 200:9, 200:13, 217:22, 218:19, 218:20, 228:3, 241:11, 243:13, 284:14, 293:4, 293:5, 293:7
transmissions
193:16
transmit
12:22, 13:11, 13:22, 14:12, 240:9, 242:1, 274:19
transmits
240:5
transmitted
12:11, 13:7, 14:7, 241:18
transmitting
15:14, 240:15, 246:2, 250:19, 281:14
trending
271:12
trial
1:2
tried
213:1
tries
292:15
triggered
292:12
trombetta
1:22, 2:11, 296:2, 297:10
trouble
186:8
trs
243:4
true
30:6, 55:1, 57:12, 69:8, 72:2, 74:13, 75:12, 76:11, 80:16, 81:16, 90:21, 94:1, 123:14, 170:7, 198:12, 215:16, 215:20, 230:4, 295:4, 296:9
truth
140:12, 142:7
truthful
205:3
try
15:7, 44:7, 52:14, 118:8, 141:1, 147:16, 154:19, 204:22, 205:1, 205:2, 216:6, 222:17, 226:22, 227:6, 232:9
trying
14:3, 17:3, 17:9, 19:22, 20:22, 21:4, 25:5, 26:7, 27:17, 28:12, 31:3, 39:3, 45:12, 48:6, 49:4, 49:6, 56:8, 74:9, 75:6, 76:4, 78:5, 78:6, 93:14, 95:3, 95:7, 95:19, 96:4, 96:7, 105:10, 105:14, 123:2, 128:4, 143:5, 143:11, 153:19, 161:1, 162:17, 163:11, 171:3, 174:8, 188:4, 213:14, 224:15, 230:7, 230:14, 233:3, 233:6, 233:9, 238:14, 252:8, 255:12, 278:1, 278:12, 279:6, 287:19, 292:12, 293:6
tuminaro
3:3, 4:8, 5:7, 5:8, 6:6, 11:10, 15:7, 25:3, 25:8, 32:21, 35:17, 49:10, 49:14, 51:2, 83:3, 90:9, 91:8, 91:11, 97:8, 98:12, 98:18, 102:10, 102:20, 103:2, 103:3, 105:21, 106:2, 116:3, 150:16, 150:20, 150:22, 161:5, 185:16, 189:12, 197:7, 197:14, 198:12, 199:3, 202:17, 202:19, 203:2, 206:8, 206:15, 206:18, 206:21, 211:15, 211:18, 212:1, 227:13, 235:12, 235:14, 236:19, 255:19, 259:3, 259:5, 267:13, 291:9, 291:12, 294:17
tunnel
38:14
turn
52:22, 54:8, 106:4, 143:21, 157:17, 169:14, 193:7, 205:6, 217:5, 219:22, 224:9, 259:7, 260:11, 285:7, 290:12
turning
141:14, 141:21, 143:4
two
60:16, 67:7, 125:14, 138:7, 139:11, 145:1, 145:15, 147:9, 148:10, 152:3, 153:14, 154:7, 156:7, 156:13, 163:5, 163:14, 183:10, 184:17, 192:10, 201:1, 216:15, 235:19, 264:14
two-phase
138:15, 139:4
type
42:17, 44:9, 50:7, 231:6, 240:12, 241:22, 278:4
types
125:14
typically
237:15
typo
262:17

U

uncalled
197:13
unconditionally
228:2, 228:3
under
57:22, 79:3, 89:19, 130:8, 227:15
underground
67:11, 67:14, 70:17, 71:1,

71:6, 71:7, 71:9, 71:11, 84:9, 84:20, 86:1, 86:18, 88:1, 182:15, 186:21, 257:3, 258:19
underneath
61:11
understand
6:16, 13:4, 14:5, 14:16, 17:4, 17:10, 19:22, 21:1, 21:4, 26:1, 28:15, 33:3, 33:7, 37:4, 38:22, 41:4, 48:3, 73:11, 74:10, 76:4, 77:8, 77:12, 78:5, 85:5, 88:2, 91:2, 95:2, 109:11, 110:17, 111:3, 114:10, 121:3, 121:6, 121:10, 121:20, 121:22, 133:1, 143:18, 144:9, 148:1, 159:16, 162:10, 165:17, 167:7, 170:15, 171:17, 174:8, 176:1, 177:5, 187:7, 188:15, 193:1, 197:3, 197:8, 197:10, 199:4, 203:19, 208:19, 210:9, 215:6, 216:18, 223:3, 223:10, 228:9, 229:6, 229:8, 229:15, 230:2, 230:6, 230:15, 232:11, 232:14, 233:3, 233:7, 233:8, 242:12, 242:16, 242:18, 258:11, 271:9, 274:2, 278:12, 291:16, 291:22
understanding
17:4, 17:10, 43:17, 155:10, 155:12, 185:8, 226:20, 227:10, 239:16, 269:4, 294:14
understood
113:8, 220:4, 288:21
uninteresting
108:13, 113:20, 114:19, 114:20, 118:17, 118:21, 188:18, 189:2, 189:9, 203:12
unique
269:14
united
1:1
unix
168:4
unknown
55:17, 125:9, 126:3, 254:22, 267:1
unless
10:4, 23:15, 80:22, 82:11, 87:15, 129:21, 285:4
unrelated
187:13
untenable
150:11
until
152:20, 155:9, 167:9, 275:17
update
15:17, 47:16, 48:12, 49:19, 50:2, 50:14, 50:17, 128:16, 129:6, 129:9, 129:14, 129:15, 129:17, 130:2, 130:14, 130:22, 131:1, 131:13, 132:15, 135:2, 135:5, 135:10, 135:11, 137:2, 138:16, 138:22, 139:3, 139:14, 139:15, 139:18, 140:9, 140:11, 141:16, 143:16, 147:8, 147:17, 151:15, 154:20, 154:22, 155:1, 155:6, 155:9, 156:14, 156:20, 158:19, 158:20, 159:2, 160:9, 160:10, 160:13, 162:20, 165:8, 166:9, 168:6, 168:7, 169:3, 169:15, 170:4, 170:19, 171:11, 172:20, 254:4, 281:17
updated
70:5, 126:18, 126:21, 128:2, 128:6, 128:11, 128:16, 129:4, 132:5, 133:9, 133:22, 134:7, 135:17, 148:1, 148:5, 149:8, 153:21, 155:2, 155:7, 156:5, 156:10, 158:3, 159:12, 160:6, 161:14, 167:15, 168:1, 169:1, 170:1, 171:5, 172:8, 172:15, 172:16, 173:3, 173:10
updates
48:9, 67:12, 134:3, 134:5, 134:10, 142:14, 151:17, 154:11, 157:6, 159:4, 164:7, 169:12
updating
135:1, 135:7, 136:11, 137:11, 139:7, 139:12, 139:20, 140:8, 147:4, 147:5, 147:14, 147:15, 148:2, 148:21, 152:14, 153:16, 154:2, 154:10, 155:18, 155:21, 156:1, 157:15, 158:8, 161:18, 161:21, 161:22, 162:2, 162:9, 165:14, 166:11, 167:13, 169:7, 169:8, 170:3, 170:18, 171:19, 172:11, 172:21, 172:22, 173:13, 173:14, 174:3, 174:5, 285:1
usage
234:5
usbs
186:14
use
8:4, 23:18, 28:21, 28:22, 29:17, 32:16, 40:13, 58:7, 60:11, 60:12, 71:8, 71:11, 86:4, 87:17, 92:17, 94:18, 96:4, 97:19, 99:4, 112:7, 126:15, 134:12, 147:7, 147:17, 147:18, 168:9, 170:1, 173:8, 173:9, 175:11,

175:14, 175:17, 176:2, 176:9, 179:18, 188:7, 188:10, 191:15, 205:13, 223:2, 224:13, 234:6, 234:7, 238:15, 243:4, 251:1, 251:16, 251:17, 257:2, 287:18
useful
74:17, 75:11, 203:14, 237:11, 238:8, 270:7
user
190:15
uses
37:1, 112:3, 138:7, 151:11, 228:1
using
38:10, 38:19, 38:20, 40:11, 40:17, 41:8, 41:21, 43:20, 44:20, 53:9, 63:19, 67:4, 86:16, 86:17, 112:17, 129:2, 129:3, 129:8, 131:4, 137:8, 148:22, 155:16, 159:7, 159:11, 161:17, 164:20, 169:16, 186:19, 213:21, 224:20, 241:6, 241:10, 251:10, 252:7
utilize
34:12, 35:3, 36:21, 169:4, 268:11, 272:2
utilizes
37:11, 42:2, 239:20, 270:12
utilizing
269:17
utterly
211:19

V

valid
193:14
variety
103:17
various
29:6, 34:5
vcr
182:8, 182:9
vectors
86:10, 87:5, 88:19, 89:11, 89:21, 90:12
vein
69:22
vendors
276:6
verify
48:11
version
248:13, 250:4
versus
89:1, 129:3, 132:11, 132:15, 133:17, 137:10, 213:8, 218:3, 284:2
via
38:13
view
38:16, 50:7, 104:18, 119:10, 119:11, 187:11, 241:3
views
103:12
violating
73:9
virus
180:11
viruses
181:13
visit
183:12, 183:22, 191:2
visiting
181:18
voice
197:12, 197:14, 206:20
volume
40:20, 41:20, 272:4, 274:6
vpn
241:12

W

wait
44:13, 69:4, 142:20, 168:22, 169:4, 169:20, 292:14
waiting
149:6, 150:9
wall
53:11
wang
3:12
wanted
96:21, 98:13, 98:16, 98:19, 190:18
wants
158:20, 198:6
washington
3:7
watch
182:10
way
23:18, 26:22, 82:10, 90:5, 95:16, 102:16, 104:14, 124:18, 126:6, 128:14, 130:12, 142:14, 161:13, 162:7, 162:8, 162:9, 168:13, 174:6, 179:5, 182:12, 187:13, 188:3, 198:11, 207:17, 222:5, 222:22, 229:14, 241:9, 243:14, 243:22, 248:7, 263:19, 265:2, 270:16, 281:18, 284:10, 291:22, 293:12, 294:2, 296:21
ways
80:20, 81:19, 82:14, 83:10, 83:11, 94:9, 109:13, 111:6, 151:12, 167:20, 168:21, 169:19, 169:21
we'll
78:11, 145:17, 246:4, 255:18
we're
36:1, 56:15, 63:22, 73:10, 90:14, 91:7, 96:10, 188:7, 189:5, 211:20, 225:3, 225:10, 265:9, 294:18
we've
102:17, 150:14, 202:21
web
46:9, 182:7
website
180:11, 180:16, 180:17, 183:9, 183:12, 183:21, 184:1, 184:19, 185:1, 191:10, 191:16, 192:2
websites
183:4, 184:11, 190:17, 192:11
weird
149:12
welcome
51:6, 106:3, 151:1, 212:2, 259:6, 291:13
well-considered
55:16, 254:21
well-known
48:14, 111:20,

114:22, 162:22, 181:11, 192:19, 214:20, 233:17, 233:21
wenke
1:13, 2:1, 4:4, 23:7, 24:22, 78:10, 96:10, 124:4, 198:10, 236:3, 279:4, 295:2, 296:5, 296:14
went
48:16, 48:18, 188:20, 188:21, 200:7, 249:7, 256:18, 268:3, 271:4, 274:1
whatever
44:10, 67:12, 73:20, 74:10, 76:17, 77:9, 77:10, 79:3, 79:12, 79:13, 80:6, 87:18, 92:5, 101:10, 102:5, 116:11, 126:2, 134:16, 140:16, 141:8, 144:12, 147:21, 161:16, 161:20, 162:19, 168:4, 168:10, 172:13, 176:9, 185:5, 186:22, 187:16, 197:20, 213:3, 262:16, 277:22
whenever
48:13, 161:15
whereas
195:13, 266:9
wherein
9:15, 35:11, 35:13, 107:5, 194:4, 194:6, 199:15, 199:17, 202:9, 226:14, 263:21
whereof
297:2
whether
17:6, 17:8, 21:16, 76:10, 90:6, 90:10, 91:4, 91:5, 91:12, 112:2, 112:14, 120:13, 120:21, 123:12, 130:13, 131:10, 131:12, 133:5, 134:4, 134:5, 155:22, 169:20, 187:17, 195:21, 217:21, 238:1, 238:3, 239:7, 243:12, 248:4, 248:5, 250:5, 261:17, 263:7, 263:17, 264:6, 278:12, 293:20
white
125:2, 125:8, 237:17, 238:19
whole
29:8, 30:10, 41:17, 66:12, 73:8, 74:1, 75:18, 94:5, 94:6, 110:13, 125:8, 150:2, 154:1, 168:11, 168:12, 225:4, 288:12
wide
136:22
widely
65:15
window
50:5, 166:20
wise
43:11, 60:22
wish
274:13
withdraw
139:8, 139:9, 139:19, 140:1, 140:3
withdrawing
49:8, 49:12, 161:3, 206:11
withdrawn
140:16
within
18:21, 22:11, 232:11, 232:14, 262:8, 263:2, 267:1, 296:3
without
47:14, 70:20, 75:2, 87:18, 88:22, 90:2, 112:17, 129:13, 130:10, 132:20, 132:21, 135:19, 137:2, 141:13, 141:21, 144:19, 155:18, 162:2, 182:17, 207:1, 256:19
witness
4:2, 5:3, 15:11, 25:2, 25:5, 78:12, 124:6, 197:12, 198:22, 199:2, 206:14, 207:1, 211:16, 211:21, 279:5, 296:5, 296:9, 297:2
word
23:17, 180:11, 180:13, 181:2, 251:1, 251:14, 251:16, 251:17, 278:9
words
14:15, 14:16, 32:16, 64:1, 95:7, 95:11, 95:13, 96:1, 96:4, 101:16, 123:3, 158:6, 175:16, 175:19, 287:1, 287:10, 289:11
work
45:6, 48:16, 48:18, 64:12, 99:17, 128:7, 132:17, 133:21, 150:6, 153:16, 168:17, 174:5, 183:7, 191:3, 195:17, 220:19, 233:18, 274:14, 285:4
worked
43:19, 92:12, 282:10
workflow
94:6
working
47:12, 50:1, 156:6, 156:8, 156:16, 213:8, 213:9, 242:6
works
30:1, 33:8, 62:6, 83:9, 94:8, 161:2, 161:11, 165:18, 171:18, 209:20
world
53:7, 186:21, 257:3
worry
74:8, 74:20, 164:15, 164:18
worthwhile
234:11
wouldn't
44:19, 100:11, 100:12, 173:4, 173:5, 175:21, 183:2, 185:6, 187:11, 191:5, 253:4
wow
60:16, 79:3, 137:3, 140:20, 179:14
write
63:20, 142:21,

144:9, 145:21, 146:3, 146:11, 146:22, 148:12, 149:15, 160:16, 166:4
writes
152:4, 168:5
writing
144:13, 144:14, 144:18, 152:8, 153:2, 153:5, 154:14, 154:16, 157:5, 161:8, 163:17, 166:16, 288:21
written
20:20, 22:4, 23:20, 90:17, 102:8, 162:10
wrong
30:9, 40:20, 95:8, 96:13, 206:2, 266:3
wrote
54:20, 55:5, 205:12, 288:3

X

x----------
--
4:1
x-force
66:2, 67:7, 67:9, 70:10, 70:12, 70:19, 72:5, 72:14, 84:3, 84:7, 84:10, 85:18, 86:8, 86:15, 86:17, 87:3, 87:16, 87:22, 88:2, 88:17, 89:1, 89:3, 89:10, 89:19, 90:10, 91:21, 91:22, 92:1, 93:5, 94:9, 94:11, 256:15, 257:1, 257:4, 257:13, 258:16, 258:18
x-force's
84:19

Y

years
50:8, 85:12, 88:10, 92:13
york
1:14, 2:7, 2:12, 3:6, 3:15, 101:9, 296:3, 296:15
yourself
28:17, 28:20, 50:13, 155:5, 182:10

Z

zero
140:1

.

.2025
297:5
.2600
3:8
.3000
2:8, 3:16

0

00889
1:6
01324
54:3, 204:19, 205:9, 215:13, 235:10

1

10
169:16, 172:12, 196:1, 241:10, 244:20, 254:6
10.07
297:5
100
18:18, 139:8, 139:9, 139:10, 140:1, 140:3, 141:6, 169:15, 172:11, 291:19, 292:10, 292:11, 293:7, 293:9, 293:14, 294:3
1001
6:12
10036
2:7, 3:15, 296:16
1004
216:22
101
34:10, 34:19, 190:3, 190:7, 190:12
102
293:14, 294:3
1037
52:16, 57:6, 65:10, 247:2, 247:3, 247:5, 247:14, 247:17, 248:3, 248:6, 248:20, 249:4, 249:20, 252:22, 253:12, 255:2, 255:21, 256:2, 257:12, 273:5, 273:20, 282:13
104
285:7, 285:9, 293:14, 293:15, 293:19, 294:3, 294:8
107
5:17
11
125:6, 244:22, 254:6, 277:11
110
219:22, 220:3, 225:4
1100
3:6
114
224:9, 224:12, 225:4, 230:16
116
271:12, 293:22
12
37:19, 37:22, 38:5, 41:6, 41:10, 174:21, 175:2, 271:1, 271:5, 277:13
122
239:15
124
251:4, 251:6, 251:13
126
245:9, 250:15, 251:2, 251:14, 251:18
13
277:13, 277:14, 290:12
1324
235:6
142
262:3, 264:21, 265:11, 265:18
143
259:7, 259:8, 259:10, 259:12, 259:13, 262:3, 262:7, 262:13, 264:20, 265:18, 266:1
144
262:4, 264:20, 265:12, 265:18
15
39:4, 271:6
16
33:14
17
205:6, 205:11, 210:6, 210:15, 215:13, 215:21
18
24:17, 24:18, 25:18, 26:22, 27:12, 27:13,

27:18
19
70:2
1980
233:20
1990
29:13, 40:12, 43:1, 44:5, 44:19, 48:15, 48:16, 49:17, 70:2, 233:17, 276:13
1996
70:3
1998
28:12, 53:7
1999
233:18
1a
9:4, 27:4, 27:16
1b
9:12, 15:21, 30:13, 30:17, 31:7, 33:21, 37:8, 106:8, 107:2, 108:3, 113:4, 113:18, 114:2, 116:21, 121:17, 122:4, 122:6, 122:16, 126:7, 176:12, 177:15, 194:1, 194:9, 194:10, 196:22, 198:2, 198:18, 199:8, 199:13, 200:15, 200:18, 200:20, 201:17, 201:18, 203:10, 204:7, 208:2, 208:8, 208:10, 208:17, 209:2, 209:19, 209:20, 210:2, 210:21, 210:22, 211:1, 211:6, 212:12, 213:3, 214:12, 214:15, 221:2, 221:3, 221:10, 221:13, 221:21, 222:6, 222:8, 223:5, 223:8, 227:9, 228:8, 228:14, 228:19, 229:19, 229:20, 231:9, 240:1, 265:4, 267:11, 267:21, 269:10, 269:19, 270:17, 271:1, 271:10
1c
12:16, 14:5, 14:11, 15:15, 31:10, 97:17, 177:14, 177:15, 239:1, 239:2, 240:4, 243:12
1d
15:21, 16:9, 16:15, 17:1, 46:9
1e
45:13, 46:22, 47:2

2

20,000
34:12, 35:3, 36:21, 41:21, 268:11, 269:17
2000
40:13, 48:15, 48:17, 49:17, 55:22, 56:21, 158:1
20005
3:7
2001
54:2
2009
37:18, 37:21, 41:11, 46:1, 271:1
2010
194:13
2012
45:19, 46:5, 47:3
2016
5:10
2019
54:3, 204:19, 205:9, 215:13, 235:10
202.371
3:8
2020
117:15, 119:20, 194:14
2023
1:6
2024
1:15, 5:20, 296:16, 297:4
2030
117:16, 119:22
21
5:20
210
275:12, 283:12
212.969
2:8, 3:16
213
19:11, 26:15, 30:21, 31:5, 34:3, 34:4, 268:4, 280:18, 284:7
214
24:6, 25:9, 25:14, 26:7, 26:20, 27:2, 27:7, 30:21, 34:10, 34:17, 36:17, 36:19, 41:19, 45:5, 268:10, 271:2
215
28:8
217
266:12, 266:13, 266:15, 266:16
218
271:19
219
274:21, 275:1, 276:9, 276:17, 278:2, 278:10, 278:16, 279:15
220
31:1, 115:7
223
285:16, 286:4, 289:12
224
286:4
227
285:16, 289:12
228
84:2
23
193:7
230
115:9
237
57:9
24
58:9
25
22:11, 193:13
250
115:10
27
31:2, 54:16, 54:20
276
52:22, 57:7, 57:8, 57:18
277
57:18, 67:15, 79:2, 79:14, 79:21, 83:19, 273:5, 273:20
278
103:4, 256:1
279
66:1, 66:15, 71:20, 85:5, 256:22
29
226:10, 226:18, 227:4, 227:7,

227:11, 227:15, 228:16, 235:13, 235:15, 235:17, 235:18, 235:21
297
1:21
2a
101:19

3

3
217:18, 218:10
30
50:8, 85:12, 88:10, 92:13
31
179:4, 226:18, 227:4, 227:7, 227:11, 228:20, 229:1
32
157:19, 158:14
35
229:5
36
179:20
37
292:3

4

4
294:19, 296:17
41
179:5, 240:2
44
260:12, 260:14, 260:17, 260:20, 262:1, 262:2, 262:10, 262:22, 264:9, 266:2, 266:4, 266:6, 266:7
45
261:12
46
266:2, 266:4, 266:7, 294:19, 296:17

5

5,884,033
217:1
50
240:3, 241:9
51
108:10, 109:10, 111:3, 112:11, 114:10, 118:5, 188:22
531852
1:20
55
115:6, 117:13, 119:19
58
1:16, 245:6, 245:8, 296:17

6

60
54:8, 54:12, 54:15, 54:16, 54:19, 55:19, 57:4, 126:16, 254:14, 254:19, 255:6
61
56:4, 255:7
641
6:12, 6:15, 6:18, 11:6, 19:17, 20:16, 25:12, 27:4, 30:14, 31:10, 33:14, 33:21, 37:8, 45:13, 53:21, 54:5, 56:4, 75:19, 99:4, 106:4, 106:11, 107:10, 108:1, 108:4, 108:18, 109:15, 111:11, 111:13, 111:21, 112:21, 113:22, 115:2, 115:14, 115:16, 116:4, 116:14, 116:20, 117:6, 118:4, 122:12, 124:13, 125:13, 126:6, 126:11, 157:14, 157:22, 158:13, 159:1, 159:13, 164:13, 171:9, 175:10, 175:13, 179:9, 188:16, 189:7, 194:12, 195:12, 196:13, 196:22, 205:13, 221:18, 221:21, 223:3, 226:9, 231:5, 231:14, 240:19, 241:16, 242:3, 247:20, 247:21, 248:17, 250:7, 253:6, 253:10, 253:16, 253:20, 254:5, 255:8, 255:13, 255:16, 267:11, 267:21, 268:22, 270:16, 277:4, 277:5, 277:16, 279:13, 280:13, 286:16, 289:1
65
235:7, 235:8, 235:15, 235:18, 293:18
67
259:11, 259:12
6a2c
261:8, 261:18, 262:21, 263:1, 263:8, 263:17, 264:7, 264:14, 264:22, 265:19
6a2d
261:13, 264:22, 265:19
6a5
260:1, 260:5, 262:14, 262:15
6a7
262:16, 262:19

7

7,895,641
1:8, 6:13
70
126:16

8

8
1:16, 296:17
80
44:20
8299
2:7, 3:15, 296:16
889
259:10
8th
297:3

9

90
43:19, 48:2, 50:22, 51:8, 51:12, 56:18, 56:21, 59:2, 69:19, 128:1, 128:10, 130:2, 130:14, 132:3, 133:7, 134:6, 151:6, 181:9, 181:10, 182:13, 182:14, 234:7