

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS

UNITED STATES OF AMERICA,)
)
Plaintiff,)
)
VS.) CASE NO. 5:15-CR-50087
)
ANTHONY ALLEN JEAN,)
)
Defendant.)

TRANSCRIPT OF MOTION HEARING
BEFORE THE HONORABLE TIMOTHY L. BROOKS
October 11, 2016; 2:14 p.m.
FAYETTEVILLE, ARKANSAS

FOR THE GOVERNMENT:

Mr. Denis Dean
United States Attorney's Office
414 Parker Avenue
Fort Smith, AR 72901
(479) 249-9040
Denis.Dean@usdoj.gov

FOR THE DEFENDANT:

Mr. Jose Manuel Alfaro
Federal Public Defender
3739 N. Steele Blvd., Suite 280
Fayetteville, AR 72703
(479) 442-2306
joe_alfaro@fd.org

Proceedings recorded in realtime via machine shorthand.

Dana Hayden, CCR, RMR, CRR
Federal Official Court Reporter
35 East Mountain Street
Fayetteville, Arkansas 72701

1	I N D E X	
2	(MOTION HEARING)	
3		
4		Page
5	October 11, 2016	
6	Procedural History by the Court	3
7	<u>DEFENDANT'S WITNESSES</u>	
8	DR. MATTHEW MILLER (via videoconference)	
9	Direct Examination by Mr. Alfaro	20
	Cross-Examination by Mr. Dean	42
10	Redirect Examination by Mr. Alfaro	51
	Examination by the Court	52
11	Redirect Examination by Mr. Alfaro	67
12	<u>GOVERNMENT'S WITNESSES</u>	
13	DANIEL ALFIN	
14	Direct Examination by Mr. Dean	70
	Cross-Examination by Mr. Alfaro	86
15	Examination by the Court	95
16		
17	Closing Argument by Defendant	100
18	Closing Argument by Government	113
19	Motion taken under advisement	118
20	Court Adjourned	123
21	Court Reporter's Certificate	124
22		
23		
24		
25		

1 THE COURT: We are proceeding in the matter of
2 the United States versus Anthony Allen Jean. Our docket
3 number is 5:15-CR-50087, defendant number 1. Denis Dean
4 appears on behalf of the United States. Joe Alfaro
5 appears on behalf of Mr. Jean.

6 Good afternoon, Mr. Jean.

7 THE DEFENDANT: Good afternoon.

8 THE COURT: We are proceeding today in a motion
9 to compel hearing. For some background, Mr. Jean is
10 facing a superseding indictment that was filed on June
11 22nd, which charges him with four counts involving the
12 receipt of material involving the sexual exploitation of
13 a minor, one count involving possessing material
14 involving the sexual exploitation of a minor, and one
15 count of accessing the Internet with intent to view
16 child pornography. There's also a forfeiture
17 allegation.

18 For background purposes, the Court would like
19 to incorporate by reference certain background
20 information in the nomenclature that it has used in
21 stating the findings from its prior order on the
22 defendant's motion to suppress. The Court's order can
23 be found at document number 40 of the case file.

24 As I said, the current motion before the Court
25 involves the defendant's motion to compel discovery. I

1 understand that the defendant anticipates calling an
2 expert witness in the field of computer coding, or
3 whatever the proper terminology would be, forensic
4 computer codes, and that witness is going to be
5 appearing via teleconference, and I assume that that is
6 the gentleman on our TV screen.

7 And, sir, you would be Mr. Matthew Miller. Is
8 that right?

9 MR. MILLER: That is correct.

10 THE COURT: All right. And I understand that
11 the government would intend to call, during this
12 hearing, one of the FBI agents that has had to do with
13 this particular investigation in Mr. Jean's case
14 specifically, but it also involves a number of cases
15 across the country and that would be Agent Alfin, who we
16 anticipate testifying live. Is that correct?

17 MR. DEAN: Yes, your Honor.

18 MR. ALFIN: Good afternoon, your Honor.

19 THE COURT: Good afternoon, Mr. Alfin.

20 All right. Well, before proceeding to take up
21 evidence on our motion, I would like to state the
22 Court's understanding of the present posture of this
23 discovery dispute in terms of what information the Court
24 has provided, as contrasted with the information that
25 the government hasn't or won't provide.

1 This information is largely gleaned from the
2 parties' motion. Mr. Alfaro's motion appears at
3 Document 28 of the court file. The government's
4 response was at -- or appears at Document 30 of the
5 court file, and there are many attachments and even a
6 supplement that the parties have filed, including
7 letters and e-mails that counsel has exchanged back and
8 forth.

9 The parties have also attached affidavits to
10 their papers. The affidavits would include a prior
11 affidavit from Mr. Miller, who we anticipate testifying
12 live in this case, but also an affidavit from Agent
13 Alfin, who's testified in another, but similar, case.

14 And what I have observed in reading your briefs
15 and the affidavits and being aware of the expert
16 testimony that the parties mutually put on at our
17 suppression hearing, there seems to be a little bit of a
18 disconnect in the terminology that has been used to
19 describe the information -- the universe of information
20 that exists and which portion of that universe has not
21 been produced or is the object of the defense motion to
22 compel.

23 So what I'd like to do in explaining a little
24 bit further some of the necessary background is to put
25 that -- is to use the terminology that I understand or

1 to use the nomenclature that the Court has used in its
2 prior order that is helpful to the Court in
3 understanding the different components, which is
4 somewhat different than the nomenclature that the
5 defense experts have used in describing what they call
6 the four components of a NIT.

7 So I'm trying to get everyone on the same page
8 so that we have our terms defined and we know what we're
9 talking about, or at least that I understand what is in
10 dispute.

11 So it begins with what we call the government's
12 NIT, or the FBI's NIT, which is short for a network
13 investigative technique. In this case the FBI's NIT
14 consisted of computer code, which the Court understands
15 is basically a string of computer instructions or
16 commands, which were sent to activating users' computers
17 who logged into and/or downloaded, allegedly, child
18 pornography from what has been described as the Playpen
19 website while it was under the government's control. In
20 this case the activating computer user logged in with
21 the avatar "regalbegal."

22 According to the government, when regalbegal
23 began to download child pornography, the NIT -- which,
24 again, is computer code -- and what we might call the
25 NIT's operating instructions, were sent to regalbegal's

1 computer.

2 Those instructions ran on that computer and
3 caused that computer to send back to the government six
4 pieces of identifying information as itemized in the
5 Court's suppression order and included, among other
6 things, a unique identifier code that was transmitted by
7 the NIT but then other information that was specific to
8 regalbegal's computer, including that computer's
9 specific MAC address and hostname, as well as
10 regalbegal's computer's operating system and some other
11 identifying information like that.

12 These pieces of information were then sent back
13 in what has been described as "clear text," which I
14 understand to mean in an unencrypted fashion, back to
15 the government's computer.

16 According to prior testimony at the suppression
17 hearing, the NIT did its business in sending this
18 information back to the government within a span of 0.27
19 seconds. And very importantly, according to the expert
20 testimony provided by both the government's expert and
21 the defense expert at the suppression hearing, this
22 information that was collected from Mr. Jean's computer
23 was sent back to the government via the regular
24 Internet, which is as opposed to the Tor browser, and
25 the intentional side effect of sending it back over the

1 regular Internet was that every, what has been described
2 as quote/unquote packet of information sent from
3 regalbegal's computer back to the government's computer,
4 those packets had regalbegal's true IP address attached
5 to the packets.

6 So the government then submitted an
7 administrative subpoena to the Internet service
8 provider, as known as an ISP, that was associated with
9 the IP address that was on these packets of information
10 received from regalbegal's computer.

11 With the administrative subpoena, they obtained
12 regalbegal's IP subscriber information, and with that
13 information, it led them directly to Mr. Jean's
14 doorstep, where a search warrant for Mr. Jean's
15 computers was executed.

16 The Court understands, although not super
17 deeply, but the Court understands that in a noncustodial
18 interview, either incident to the execution of the
19 search warrant or since that time, the government
20 contends that Mr. Jean has admitted to downloading the
21 child pornography that is in question in this
22 indictment.

23 Mr. Jean's -- given Mr. Jean's admission in
24 this regard, the Court is uncertain of any remaining
25 evidentiary need or value to these other six pieces of

1 information that were collected from Mr. Jean's
2 computer.

3 Following Mr. Jean's arraignment on the initial
4 indictment, the defense asked for discovery, and after
5 several back-and-forth communications between counsel,
6 the Court understands that the government has at this
7 point produced the following: Number one, what I refer
8 to and understand to be known as the complete NIT
9 computer code, which is to say, more specifically, the
10 operating instructions that were sent to Mr. Jean's
11 computer when he began downloading the child pornography
12 as alleged by the government, which in this case caused
13 Mr. Jean's computer's specific information and
14 accompanying IP address to be sent back to the
15 government as I've described.

16 Secondly, the government has produced what has
17 been referred to as the two-way data stream between the
18 government's computer and Mr. Jean's computer as the NIT
19 instructions ran on and were executed by Mr. Jean's
20 computer.

21 Third, the government has disclosed information
22 from its own computers which detail the images allegedly
23 downloaded by the user known as regalbegal, which the
24 government now contends is Mr. Jean.

25 Number four, the government has turned over the

1 contents from Mr. Jean's computer, which it contends to
2 be the contraband evidence it seized pursuant to the
3 residential search warrant. Additionally the Court
4 understands that the government may have turned over
5 other evidence which is not necessarily related to the
6 NIT or otherwise in dispute in this case.

7 To the Court's understanding, there is only
8 really one piece of information which is in dispute,
9 which is the means and method by which the FBI was able
10 to exploit the Tor browser software that was utilized by
11 regalbegal when regalbegal accessed the Playpen website.

12 This means and method that the FBI utilized
13 allowed it to pass the NIT computer code through what
14 has been described as or analogized as a quote/unquote
15 locked door on the Tor browser such that the NIT's
16 computer code and instructions could be run on
17 Mr. Jean's computer.

18 The terminology that I understand this means
19 and manner to be known as is an exploit, and there was
20 information at our last hearing on the suppression issue
21 where this was described as the exploit.

22 It is believed that the exploit is, in itself,
23 a piece of software or, in other words, more code,
24 which, unless one of the parties objects, I'm simply
25 going to refer to that piece of software or that code as

1 the exploit code.

2 The government refuses to produce the exploit
3 code. Number one, the government contends that under
4 Rule 16, this information is not discoverable because it
5 is not material to Mr. Jean's defense. As to that
6 objection, the defendant has the burden to establish the
7 materiality of the information that it seeks in
8 discovery.

9 As a secondary matter, the government takes the
10 position that should the Court find the exploit code to
11 be quote/unquote material to Jean's defense, then in
12 that event, the government is asserting what's known as
13 the law enforcement privilege. It cites the
14 government's need to prevent disclosure of the exploit
15 code because it constitutes sensitive investigative
16 tools and techniques. To the extent that we get to that
17 assertion of privilege, it would be the government's
18 burden to establish that it applies, given the facts and
19 issues that are presented here.

20 Against that background, Mr. Alfaro, can you,
21 before we get into your -- before we get to Mr. Miller,
22 categorically what information, other than the exploit
23 code, do you seek from your motion?

24 MR. ALFARO: Thank your Honor. I'll clarify
25 what I think the Court has been requesting.

1 First I would clarify that the Court made a
2 statement that we're requesting the complete NIT
3 computer code, and I would like to clarify that what we
4 are requesting is the source code for all data that was
5 used to identify Mr. Jean.

6 Part of that would include the NIT code and so
7 Dr. Miller will clarify me if I'm wrong during his
8 testimony, but the format that I would like to lay out
9 is the testimony, I believe, will be that in order for
10 the NIT to do what it did, first there is a part of the
11 software --

12 THE COURT: Let me interrupt you because we're
13 already -- you're already confusing me with your
14 terminology.

15 MR. ALFARO: Yes, sir.

16 THE COURT: I understand that as a blanket for
17 your client's benefit and for the benefit of your
18 defense that you want to be sure that the government
19 knows that they -- that the defense wants everything,
20 the entire code, but I don't know how to make the
21 government give you specifically what you think exists
22 unless we break that down as to what that means.

23 MR. ALFARO: Yes, Judge, and so --

24 THE COURT: And my understanding, when I use
25 the term "the NIT code" or "the NIT instructions," my

1 understanding from what the government has represented,
2 that this NIT code that was -- that they ran on an
3 activating computer's computer, in its entirety, has
4 been turned over, which is separate and apart from the
5 code that they may have ran in order to get access
6 through the so-called locked door of the Tor browser to
7 allow the NIT code to run.

8 So it could be that in the way that one expert
9 looks at the entirety of the quote/unquote source code,
10 that could include both of those things and it could
11 include the data that was exchanged back in forth; it
12 could include a lot of things. But what I understand is
13 that the government has produced the code, the NIT code
14 that was run on regalbegal's, i.e., Mr. Jean's,
15 computer. And when I say the word "complete," my
16 understanding is that that is code that you or your
17 experts could run on another computer to test its
18 characteristics and abilities.

19 Secondly, I understand that the government has
20 provided to you the clear text data that was exchanged
21 as Mr. Jean's computer was communicating with the
22 government's computer so that you can take the code, the
23 NIT code, and you can take this communication from
24 Mr. Jean's computer back to the government and determine
25 whether or not it sent from Mr. Jean's computer what the

1 code was designed or engineered to do in the first
2 place. And you don't have that in the generic sense,
3 but you have the actual transmission of data between the
4 government computer and Mr. Jean's computer.

5 Separate and apart from the NIT that ran, I
6 understand that the government monitored and that its
7 computers tracked the actual images or web pages within
8 the Playpen website that regalbegal downloaded. And
9 then you have obviously the information that they
10 harvested incident to the residential search warrant.

11 So if we take the universe of all available
12 information and we subtract the things that I've just
13 described, what is left that you need, or that you're
14 seeking?

15 MR. ALFARO: Your Honor, we are seeking the
16 code that we believe the government has that was used to
17 create the NIT, not what the NIT does but what was used
18 to create the NIT and create what experts call as the
19 unique identifier.

20 This unique identifier is created by an
21 algorithm that they're associating with a username and
22 so when they are receiving this information back, they
23 are saying "We know it's correct because this unique
24 identifier we've already put into this username." What
25 we don't know is how that information was being

1 collected, stored and created, and Mr. Miller will talk
2 about why that's important.

3 So we are requesting all of that code that, the
4 terminology where using is the code that generated the
5 payload and creates this unique identifier that's being
6 used to link the defendant and the information that is
7 receiving to the defendant.

8 THE COURT: Okay. From what you've just said,
9 I understand that in addition to the things that --
10 well, first of all, do you dispute that the government
11 has turned over the code and other pieces of information
12 that I've identified?

13 MR. ALFARO: Judge, they've turned over a code,
14 but it's not the code that we've asked for, and
15 Mr. Miller will testify about what he's been able to do
16 with what the government has turned over and what he has
17 not been able to do with what the government has turned
18 over. I don't think I'd be able to address that more
19 specifically without his testimony.

20 THE COURT: Okay. So in addition to some
21 aspect of what you are calling NIT code -- which is
22 going to cause me confusion unless Mr. Miller can
23 clarify that, which I'm sure he can -- you are also
24 seeking whatever code has been used to generate this
25 so-called unique identifier which, from my starting-out

1 understanding, is some sort of number or identifier that
2 the NIT sent to run on regalbegal's computer and then
3 returned that number along with the other pieces of
4 information so that the government could match up that
5 it had sent this information to this particular
6 computer, and it could match up the results that were
7 harvested from that particular computer.

8 MR. ALFARO: I believe so. I think another way
9 to -- I guess another way to explain it is when -- I use
10 the term "payload." That is what our experts use
11 synonymously with what the government calls the NIT.

12 So there's a piece of software that, when
13 it's -- when the government was getting ready to execute
14 the NIT, or payload, it used computer software to
15 generate an algorithm to create a unique identifier with
16 this NIT.

17 So it could say we're going to send this
18 information out with a number and we get it back with a
19 number and that's how we're going to compare what we
20 sent out and what we get back. And Dr. Miller will
21 clarify that if I'm speaking different in here.

22 So what we're asking for is that code as well,
23 and Dr. Miller will explain why that's necessary.

24 THE COURT: What about the exploit, what I've
25 described as the exploit code? You're not asking for

1 that anymore?

2 MR. ALFARO: We are, Judge. We're asking for
3 three parts of a four-part code. If I can give you
4 an umbrella, the NIT is only one part of what we believe
5 is a four-part, total grouping of information. In order
6 for the NIT to do what it did, there is a series of
7 steps that had to occur, and Dr. Miller will --

8 THE COURT: I was hoping -- that was the whole
9 purpose that I lined out what my understanding that the
10 two sides are saying so that I could find kind of the
11 common ground and use the same nomenclature that we used
12 at the earlier hearing because if I shift and start
13 talking about payloads and all this other stuff, I don't
14 understand what that means.

15 I've read it, I've reread it, I've read it a
16 third time; still don't understand how you break out
17 payload. Does that mean how I have defined the NIT
18 operating instructions and how I have defined the
19 exploit, or does it refer to everything that happened?
20 I don't understand that. Now, it's your expert. I'm
21 sure Mr. Miller will be able to articulate it more
22 clearly than I was able to absorb it from his affidavit.

23 I get this code that generates the unique
24 organizer. I kind of get that and how that may or may
25 not have been provided, but beyond that, it sounds like

1 you're using one term as a broad term to describe
2 something that includes part of what you already
3 received.

4 MR. ALFARO: And, Judge, if I can clarify. I
5 would state that for the most part, we have received the
6 NIT code, which is synonymous with what experts in this
7 field refer to generally as a payload.

8 THE COURT: Okay.

9 MR. ALFARO: A payload is a set of instructions
10 that does something.

11 THE COURT: Okay.

12 MR. ALFARO: That would be the NIT. So we are
13 not contesting the payload aspect of it. We were just
14 going to educate the Court on that terminology.

15 Outside of the NIT, or payload, we believe that
16 there are other parts, other programs that have coding
17 that will run outside of the NIT or the payload that the
18 government has in its possession that are material to
19 Mr. Jean's case. That would include the exploit, what I
20 just referred to as the software that generates a unique
21 identifier, in addition to the server component, which
22 is basically how the government collected and stored
23 data that it received. And Dr. Miller will explain why
24 that information is also necessary.

25 THE COURT: The data that it documented as it

1 was monitoring regalbegal's activities on the Playpen
2 website?

3 MR. ALFARO: No, your Honor. The data that it
4 received from the NIT and stored to identify Mr. Jean.

5 THE COURT: Is that not the two-way data
6 stream?

7 MR. ALFARO: No, your Honor. And that --
8 Dr. Miller will testify why that is not the same thing.
9 What they received and how it is stored and collected is
10 separate from the two-way data stream, and Dr. Miller
11 will testify about that.

12 THE COURT: All right. That's helpful.

13 All right. Unless you have anything further to
14 outline as to what's in dispute, you may proceed.

15 MR. ALFARO: Thank your Honor. At this time we
16 call Dr. Miller to the stand.

17 THE COURT: All right. I'll have the clerk
18 administer the oath to you, Mr. Miller.

19 THE WITNESS: Okay.

20 THE COURT: If you'll please raise your right
21 hand.

22 CLERK CRAIG: If you could raise your right
23 hand, please.

24 (Whereupon, the witness was duly sworn.)

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

MATTHEW MILLER,

having been first duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. ALFARO:

Q. Dr. Miller, can you please state your name for the record.

A. My name is Dr. Matthew Miller.

Q. And, Dr. Miller, how are you employed?

A. I am an assistant professor at the University of Nebraska at Kearney.

Q. And what do you teach?

A. I teach computer science and cyber security.

Q. And how long have you been employed there?

A. This is my second year at the University of Nebraska at Kearney.

Q. And you're appearing on behalf of the defense today; is that correct?

A. That is correct.

Q. And you're being paid for your work and analysis in this case?

A. Yes.

Q. Can you briefly describe your education for the Court.

A. I went to the University of Nebraska at Kearney. I graduated in 2003 with a bachelor's. I then went to

1 Kansas State University and got my master's and my
2 doctorate in 2012.

3 Q. What was your bachelor's in 2003?

4 A. Computer science.

5 Q. And your master's?

6 A. Computer science.

7 Q. And your Ph.D.?

8 A. Computer science.

9 Q. In addition to your position as an assistant
10 professor, can you summarize for the Court your work
11 history?

12 A. So while I was going to school, we had children and
13 so I decided to work outside the home while I was going
14 to grad school. So I was a programmer for five and a
15 half years at a company called The Onyx Collection.

16 Q. What did you do at Onyx?

17 A. So at Onyx I programmed computer systems. So I
18 created software that would manage inventory. We
19 created an entire system to allow our customers to order
20 our product online. So it would do the entire
21 transaction, making sure that they got what they wanted.

22 Q. So would it be safe to say you're a computer
23 programmer, coder?

24 A. Yes, I was a computer programmer.

25 Q. Any other past relevant history in computer science,

1 work history?

2 A. I've also worked on several cases. I worked on the
3 Cottom case in doing reverse engineering. So that
4 was -- when I worked at Dakota State University, I
5 specialized in reverse engineering and assembly.

6 Q. Do you have any experience or training with what
7 we've used as a term "NITs"?

8 A. Yes, I have.

9 Q. Can you describe your training?

10 A. So I did training at Black Hat in order to learn how
11 to reverse engineer computer programs or take a computer
12 program where you do not have the source code and
13 analyze it in order to understand what it does.

14 I also worked for -- worked on the Cottom case,
15 where we had to reverse engineer the source code that
16 the government gave us. They lost the source code and
17 so we had to reverse engineer to verify that it did do
18 what the search warrant said. So verified that it only
19 sent back information in a search warrant.

20 Q. Can you explain what you mean when you say "reverse
21 engineer"?

22 A. So when you're given a piece of computer code,
23 initially you start off with source code, and your
24 source code is used to create binary code. And the
25 binary code is what actually runs on the computer, but

1 the source code is what a normal person would go through
2 and read and understand the flow of the software. It's
3 what you would debug it at.

4 So reverse engineering is taking this very
5 low-level code and pulling it up one level. So you can
6 kind of see what it does, but you don't get to see the
7 original source code that was used to create that
8 binary. So there's a little bit -- there's some
9 information that is lost in that translation.

10 Q. Is it more difficult to have to reverse engineer
11 something as opposed to looking at a source code?

12 A. Yes, it is. It is -- the example would be is if you
13 were given a building, it's a lot easier to understand
14 how a building is built and laid out if you look at the
15 blueprint of the building versus looking at the building
16 after it's been constructed and trying to figure out
17 where different beams are or doorways or hidden
18 compartments. So it is much more difficult to reverse
19 engineer than to just read through human-readable source
20 code.

21 Q. Going back to your experience, can you -- do you
22 have any specific certificates or training in computer
23 coding and testing?

24 A. So I don't have any as far as in coding, but when
25 you write a lot of programs, you have to learn to write

1 software in a good way. You learn how to do software
2 engineering. So those are courses that you take at a
3 university.

4 Q. So would that include things like malware analysis,
5 penetration testing, reverse engineering?

6 A. Yes, I did -- I did do those trainings when I was at
7 Dakota State University.

8 Q. You mentioned the Cottom case. Were you retained --
9 you said you were retained as an expert to do analysis
10 on a NIT used in that case?

11 A. Yes, I was.

12 Q. What did the government turn over in that case?

13 A. So in that case the government initially turned over
14 just the -- it was Flash, which is something that runs
15 on the Internet. So they gave us the Flash file and
16 then they gave us access to the servers that they used
17 in that case. And so that would have included -- that
18 did include the source code that was used to generate
19 the unique identifiers and log the unique identifiers.

20 So logging is where you just, you basically
21 write down every time something happens. You write it
22 into a file and then you can look at that later.

23 After that, they also, we requested and they
24 gave us the code that ran on the server, which in that
25 case we called Cornhusker, that logged the information

1 coming to the two-way data streams that were coming from
2 the regular Internet. So that would reveal the IP
3 addresses of the Tor users.

4 So they gave us that code also. So basically
5 all of the code that we asked for in that case they did
6 provide to us so that we could review it.

7 Q. Are you familiar with the Playpen cases arising out
8 of the use of a NIT, like this case in Mr. Jean's case?

9 A. Yes, I am.

10 Q. Can you explain how you're familiar with it? What
11 type of work have you done?

12 A. So I did do consulting in the Michaud case, which
13 was in Tacoma, Washington. There I just talked about
14 why an exploit was something that we need in order to
15 properly do the entire chain and verify all the code
16 that was run. I've also -- go ahead.

17 Q. Have you reviewed the declaration -- the expert
18 declaration submitted by the defense that would include
19 Yon Castle, yourself and Dr. Tsyklevich?

20 A. Yes, I have.

21 Q. And have you reviewed the declaration submitted by
22 Agent Alfin?

23 A. Yes.

24 Q. I'm sorry if I cut you off. Were you about to say
25 some other analysis?

1 A. There was another case, Matish, in Virginia where I
2 actually got to look at code similar to the code that
3 was in Mr. Jean's. So I actually got to look at the, as
4 we call it, the NIT code in that case also.

5 Q. Have you reviewed the documents in Mr. Jean's case?

6 A. Yes.

7 Q. And would that include the search warrant where the
8 government describes how the NIT was to work?

9 A. Yes.

10 Q. Were you able to hear the exchange that the Court
11 and I had regarding the information that the defense is
12 requesting?

13 A. Yes.

14 Q. So if it's okay with you, we'll address those
15 concerns.

16 Using your training and your experience, and
17 based upon your review of the software in this case
18 you've been provided and the documents, can you describe
19 what components would be required for the NIT to work as
20 it was supposed to work as described by the government?

21 A. So for the NIT to work, we talk about having an
22 exploit. So an exploit is a piece of software that does
23 something to a computer. It's computer code that is run
24 that modifies a system in some manner. Now, whether or
25 not that's a permanent manner or a temporary, it

1 modifies the system in some way such that additional
2 code that was sent also gets run, and we call that the
3 NIT code.

4 So I have analyzed the NIT code that was
5 provided, the binary file, and I have reverse engineered
6 that so I could understand exactly what it did.

7 Q. So when you say the NIT code, would that also be
8 what experts refer to as the payload?

9 A. Yes.

10 Q. What else would have to occur during this entire
11 process in regards to the components?

12 A. So in order to create the payload or the NIT that we
13 have, so in order to create the NIT, a unique identifier
14 was generated for each one of the users, I believe, and
15 that unique identifier had to be generated on a server
16 and put into the payload --

17 Q. When you --

18 A. -- and on that server -- go ahead.

19 Q. I'm sorry. When you say "generated on a server,"
20 what do you mean?

21 A. So in general when you are creating the website and
22 you are making identifiers for users, what you do is you
23 generate an identifier at one point and then every time
24 a particular user comes back, you reuse the same
25 identifier.

1 So the code on the server would have to
2 generate a unique identifier and save that somewhere and
3 then incorporate that into the NIT so that when the NIT
4 ran, it would send back the appropriate information that
5 it was supposed to send back.

6 So every time the NIT ran, it would have to
7 generate either a new version or what we call a cache
8 version. So it would have to generate a version of the
9 NIT specific to that user.

10 Q. And when you say a unique identifier is generated,
11 are you talking about written code?

12 A. Yeah. So generating the unique identifier is going
13 to be -- you're going to write software in order to do
14 that. You're going to write software code to do that.

15 Q. And so that's like a computer programming expert
16 that knows how to write computer code?

17 A. Yes.

18 Q. What would be the next step?

19 A. So after the NIT is created, then both the exploit
20 and the payload would be sent to the user's computer.
21 And again, there's different ways of doing this. I
22 don't have access to which way it was, but generally you
23 send both of them together.

24 The exploit runs first and then the NIT would
25 run and then the NIT would send back information to, I

1 would guess, another government server.

2 Q. What happens after that?

3 A. So when that government -- that other government
4 server receives the data, it's going to log that
5 information. So it's going to log the unique identifier
6 and the two-way data stream, or PCAP file that was
7 generated when it was sent back to the government
8 server.

9 Q. So if we had to use a term for that that the defense
10 has already used, would we call that the server
11 component?

12 A. That would be a server component, yes.

13 Q. So can you talk about what that, again, what that is
14 so we can be -- let me rephrase that.

15 So if we can start again from the beginning, we
16 have something that the defense has identified as
17 software that generates the unique identifier?

18 A. Mm-hmm.

19 Q. Is that the first step?

20 A. Yes, the first step.

21 Q. And what does that do?

22 A. Say that again?

23 Q. So can you re-explain, what does that do?

24 A. So that is the part that generates the unique
25 identifiers and logs them, as well as put them into the

1 NIT.

2 Q. And that's all --

3 A. It incorporates --

4 Q. And that's all computer code?

5 A. Yes.

6 Q. A second component is the NIT, or payload?

7 A. Yes. The NIT, NIT and the exploit are sent to the
8 user's computer and then the third step is the user's
9 computer contacts another government's server, as you're
10 calling another server, right, and it is logging the
11 information that is received via the regular Internet.

12 Q. And what's the next step?

13 A. So that would be the entirety of the process.

14 Q. The entirety?

15 A. Right.

16 Q. Did you have an opportunity to review what the
17 government has provided in this case, as in the coding
18 information that the government has provided?

19 A. Yes, I have.

20 Q. Can you please explain to the Court what the
21 government has provided you and what you analyzed?

22 A. So the government provided me with the NIT/payload.
23 So they gave me that information. They gave it to us as
24 the binary file. So that would be the actual
25 instructions that are run, but it's not, again, not the

1 way that a human would program it. So it was just the
2 computer code and then they gave me a, what's called
3 disassembly, or representation of what's in that file,
4 but it wasn't actually the source code that was used to
5 create it. Because if somebody was creating it by hand,
6 they would not write it in that method, right? It's not
7 the actual source code used to create that NIT that was
8 sent.

9 Q. Is there information that could be missing?

10 A. Yes, there could be. Because of the process of
11 taking computer code that is human-readable and
12 compiling it into binary code, there is almost always
13 necessarily a loss of information that is -- occurs.

14 Q. What else has the government provided?

15 A. They provided us with the two-way data stream. So
16 the PCAP capture which showed the information being sent
17 from a particular IP address to the government's
18 computer systems.

19 Q. To your knowledge has the government provided any
20 other code or information?

21 A. No.

22 Q. So we talked about the multiple components that
23 would be required in this universe which would include
24 the NIT being deployed. Given your training and
25 experience, can you explain why the defense would need

1 access to, the first step, the software that generates
2 the payload and injects the unique identifier?

3 A. So the software that was used to generate the unique
4 identifiers has to log that information, and I believe
5 the logging of that information is correlated to how
6 many times regalbegal visited the website, which I
7 believe is four.

8 So if that code is incorrect, there's a
9 possibility that maybe it was only one, maybe it was
10 ten, but that information could be incorrect if the
11 logging component was not properly coded.

12 Q. So you would need to check the code for errors in
13 how it was generated?

14 A. Yes.

15 Q. And why would we think there would be any error in
16 the code?

17 A. Well, computers all the time are being updated. If
18 you have a computer device of any sort, you are used to
19 the fact that the computer needs to be updated all the
20 time.

21 If you look at Windows or OS10 or your smart
22 phone, all of them are updated on a regular basis
23 because all of them are programmed by humans, and humans
24 make mistakes.

25 Now, they don't make mistakes very often,

1 right? There's millions of lines in Windows, and there
2 are a few mistakes that occur all of the time. So this
3 is an issue that happens with most softwares, that there
4 are software defects in that code, errors that occur
5 just because humans are programming them.

6 Q. Is it fairly common for there to be error,
7 unexpected errors, in code that's written?

8 A. Yes. That happens all the time. If you look at
9 examples that are in the media, all the time there are
10 software programs that are written in such a way that
11 they have unintended consequences of how they were
12 coded.

13 Q. The type of code that we're talking about in this
14 case, is it complex enough that it would have errors?

15 A. I don't know because I haven't actually viewed it,
16 but I would suppose that there is a possibility that it
17 could have errors, yes.

18 Q. Regarding this algorithm or this code that's
19 human-made for the software that creates a unique
20 identifier, is it possible that if there is an error, it
21 could associate different usernames with different IDs
22 created?

23 A. Yes, that is possible.

24 Q. Given your training and experience, can you explain
25 in your opinion why it would be necessary for the

1 defense to analyze the source code of the exploit?

2 A. So the exploit is going to take advantage of some
3 flaw in a computer system, and because computer systems
4 vary, it is possible that that exploit that was run may
5 have had some unintended consequence of it running and
6 may have, you know, inadvertently disabled a firewall or
7 inserted a certificate into the browser so that the user
8 would trust websites that they wouldn't.

9 So there are unin- -- there are possible
10 unintended consequences with running software remotely
11 on some computer system.

12 Q. So if you were able to analyze the exploit, you
13 would be able to determine whether it operated in the
14 manner that the government represents?

15 A. Yes. And that is what I did in the Cottom case. We
16 were given the source code. We went through and
17 verified that indeed the way that identifiers are
18 generated was correct, that the logging was correct and
19 we couldn't find any possible errors that were in that
20 software system to our knowledge.

21 Q. Can you explain how an exploit can alter someone's
22 computer?

23 A. So what happens is when an exploit runs, it runs in
24 a way that was not expected. So a browser anticipates
25 that something is of one type and it ends up being of

1 another and so it's going to do something unexpected.

2 Generally when you write an exploit, you try
3 and take those flaws to your advantage so that you can
4 run the code that you want to run, but it doesn't
5 necessarily go as planned. So the exploit could crash
6 the computer; it could, you know, cause some sort of
7 error. So those are definite possibilities --

8 Q. Did it --

9 A. -- that can exist in exploits.

10 Q. Can it disable computer settings?

11 A. Yeah, you could disable the firewall; it could add
12 additional certificates.

13 Q. Would that leave the computer vulnerable from
14 outside attack, third-party attack?

15 A. Yeah, so -- correct. Any computer that is on the
16 Internet, if it doesn't have a firewall, it could very
17 definitely be taken over by some remote attacker.

18 Q. And what do you mean when you say "taken over"?

19 A. So you can write computer code such that you can
20 completely control a computer from a remote location.
21 There are tools out there like Metasploit or the
22 Social-Engineer Toolkit that allow people to basically
23 remote control and do whatever they want with a computer
24 system.

25 Q. Regarding the exploit, the witness for the

1 government, Agent Alfin, previously stated in his, I
2 guess his affidavit, and I believe in a previous
3 hearing, that he's run the exploit on a computer and not
4 noticed any changes made to the computer.

5 What would be your response to that?

6 A. So my response would be it would depend on what
7 settings you were looking at. So when you run a code,
8 when you run a piece of code, it may take what we call
9 one execution path or one way of running. And it could
10 be that there are other execution paths that he did not
11 test when he was running it and so we haven't gone
12 through and looked at all those possible different
13 execution paths. We haven't looked at all the different
14 settings that could be looked into.

15 So the question would be what settings were
16 looked into, and are there other ones that were
17 unanticipated that were modified during that exploit
18 being run.

19 Q. You're referring to pathways that a code can take.
20 Can you clarify that a little bit more?

21 A. So I guess an analogy would be if you were on one
22 side of a city and you were to walk or drive to the
23 other side that there are a lot of different ways that
24 you could, you know, travel in your car. And so the
25 different pathways, he may have executed one where he

1 went, you know, just down Main Street and that was okay,
2 but if you go down a different one, it ends up that
3 we -- you know, something terrible happens, right?

4 And so when you are analyzing code, really you
5 want to look at it what we call statically or do the
6 reverse engineering and verify, okay, these are all the
7 pathways that it could take, and none of those pathways
8 did anything wrong with the computer, or bad to the
9 computer.

10 So that's what -- if I was given the exploit,
11 that's what I would go ahead and verify. And we would
12 test it against a variety of different operating systems
13 and make sure that it was -- it did indeed work as it
14 was -- as it stated.

15 Q. So by running the exploit on one computer, that
16 wouldn't be sufficient?

17 A. Correct. In software testing, you want to test all
18 of the different methods, pathways through a piece of
19 software, right? There are majors where you go through
20 and you verify all the different pathways and make sure
21 that nothing bad happens on any of those pathways and so
22 that's what -- when you talk about software engineering,
23 that's what you tend to do.

24 Q. So by running the exploit, that wouldn't reveal
25 possible design flaws or errors. Is that what you're

1 saying?

2 A. It could reveal them, but it won't necessarily.

3 There are other execution paths that may reveal

4 different defects.

5 Q. You're talking about reverse engineering and

6 analyzing code. Given your training and experience,

7 have you ever done that, analyzed software, tracking the

8 pathways and things like that? Have you actually done

9 that yourself?

10 A. Yes. I -- when I was programming, that was a big

11 part of your job. One was to talk to the users and make

12 sure you do what they want and the other one is to, when

13 you write your code, you need to check for all the

14 different possibilities and make sure you have a test so

15 you can verify that your code does work in all the

16 different situations in which you anticipate it to run.

17 And then there's always the other ones that you

18 weren't anticipating a user to do that they would do,

19 and it would, you know, possibly break things and so

20 then you'd have to fix your code and add another test

21 case to your test.

22 Q. Regarding what we are calling the server component,

23 as you previously testified to as kind of being the last

24 step in the process, given your training and experience,

25 can you explain why the defense would need to analyze a

1 server component?

2 A. So I think the reason for analyzing the server
3 component is similar to analyzing the code that ran on
4 the Playpen website is you just need to verify that the
5 data that was logged was logged in a correct manner and
6 that information wasn't duplicated because of coding
7 errors. Again, you're running code on that server; so,
8 there's always the possibility that there exist errors
9 because it is written by humans.

10 Q. So analyzing the server component, that code, can
11 you verify whether there would have been unauthorized
12 access by users also?

13 A. So that would typically be something that would be
14 inside of the operating system that would exist on
15 there. So we weren't given access to that. I don't
16 think you're asking for that. But that would be an
17 operating system sort of security measure that would
18 have to be in place.

19 Q. What about verifying the correct IP addresses logged
20 and then being linked properly? Is that part of a
21 server component?

22 A. Probably not, but that would be more on the -- so
23 all of that data would be logged and probably put into a
24 database. So it could be useful to make sure that the
25 IP addresses were logged properly. But again, that data

1 is also stored in that PCAP file. So whatever was
2 saving that would be something that we would want to
3 look at, I think.

4 Q. What was saved in the PCAP file?

5 A. Yeah.

6 Q. And what would you call that?

7 A. That would be a piece of software that was running
8 on the server.

9 Q. Running on the server component of the government's
10 server?

11 A. Yeah. There's a lot of ways of running it but,
12 yeah, that would be one method. Again, I don't have
13 access to that. So I don't know exactly how it was
14 architected.

15 Q. Is that something that you were given access to in
16 the Cottom case?

17 A. Yes, we were. We were given access to the -- all
18 the code that was used to log the information. We
19 weren't given access to the physical server because the
20 government said that was destroyed, or gotten rid of, or
21 something to that effect.

22 Q. Have you been provided that in this case?

23 A. No.

24 Q. In your training and your experience, can you
25 explain why what the government has provided to you thus

1 far is not sufficient to confirm the information the
2 government received or stored or logged is accurate?

3 A. So we have an entire system that we're using in
4 order to tie which user is associated with which
5 identifier; what the data stream was.

6 So this entire system is built all off of
7 software and, again, software has defects and so
8 analyzing it would help us to make sure that there are
9 no defects in that entire supply chain of software.

10 Q. Because if there was a defect, what would that mean?

11 A. If there was a defect, then a improper user could
12 get their information logged, it could identify them
13 more than once when maybe they only visited once, it --
14 there are a lot of different possibilities. And without
15 seeing all of the code, I can't necessarily say what
16 those all are.

17 Q. So without analyzing the code, we can't just come up
18 with every single scenario that could happen?

19 A. Correct. If we were given access to the code, we
20 would be able to much more specifically decide what are
21 the possible pathways that were bad or could have errors
22 in them.

23 Q. So would it be safe to say it's difficult to
24 articulate the defects when you don't have access to the
25 code?

1 A. That would be a good characterization, yes.

2 MR. ALFARO: I'll pass the witness, Judge.

3 THE COURT: All right. Thank you.

4 MR. DEAN: May I inquire, Judge?

5 THE COURT: You may.

6 CROSS-EXAMINATION

7 BY MR. DEAN:

8 Q. Good afternoon, Dr. Miller. My name is Denis Dean.
9 I'm an assistant U.S. attorney. We've never met before,
10 have we?

11 A. No, we have not.

12 Q. I think I passed through Kearney a couple months
13 ago. It's got the museum over it on the interstate?

14 A. That is correct, yes.

15 Q. No offense to Kearney. I just breezed right
16 through. We didn't -- I didn't stop; I didn't visit
17 with you.

18 When was the last time you were in Arkansas,
19 sir?

20 A. I think I was in Arkansas this summer. We drove
21 through on vacation.

22 Q. Did you stop anywhere of substance, like the FBI
23 headquarters in Little Rock?

24 A. No, I did not.

25 Q. Okay. So you haven't reviewed any computers or any

1 digital evidence related to this case, correct?

2 A. I have reviewed some evidence in this case. The NIT
3 and the PCAP.

4 Q. But Mr. Jean's computer and the evidence that was
5 located on it you have not reviewed?

6 A. No, I have not.

7 Q. Or, for that matter, any computer involved in
8 Playpen, in this website case that we're dealing with?

9 A. Correct, I have not.

10 Q. Okay. Doctor, to your knowledge none of the other
11 experts that have been mentioned have looked at actual
12 computers involved in this case; is that correct?

13 A. I do not believe so, no.

14 Q. I'm going to violate prosecutor 101 on cross by
15 asking this question, but why haven't you don't that?

16 A. That is not necessarily my area of expertise. I
17 don't typically do that type of forensic analysis. I am
18 more at the software level rather than analyzing a
19 computer and the file system associated with it.

20 Q. And I can appreciate that, but wouldn't there be
21 some value? Wouldn't it be helpful to actually look at
22 the computer to see if anything was altered or changed
23 or disabled?

24 A. It could be useful to look at and have a forensic
25 expert look at it who is used to looking at those types

1 of things, but again, that's not my area of expertise.
2 And the way that I believe the NIT ran and the exploit
3 ran, I don't know that they would necessarily leave
4 something that I would be able to see at this point.

5 Q. But they could?

6 A. You're right, it could, yes.

7 Q. Okay. So your expertise deals with a NIT.

8 Describe -- because I don't think I got it on direct.

9 Describe your methodology that you used to examine the
10 NIT in this case.

11 A. Can I -- let me look just a second.

12 So in this case, because this was running in
13 Linux, I had set up a Linux machine. I ran the NIT on
14 my Linux machine and then had it connect back to a
15 computer that I was in control over so that I could
16 verify that the two-way data stream that it produced was
17 consistent with the two-way data stream that I was given
18 in the PCAP file.

19 Q. And?

20 A. And it was consistent.

21 Q. Okay. Now, in your -- you issued a declaration in
22 the Michaud case out in Washington, correct?

23 A. Yes, that is correct.

24 Q. In that declaration, specifically at Paragraph 4,
25 you state that -- and I'm quoting you -- a computer

1 system that has been exploited has been fundamentally
2 altered in some way.

3 A. Correct.

4 Q. Do you recall making that statement?

5 A. Yes.

6 Q. Now, you -- and there were several people involved
7 in the Cottom case, but you helped prepare a forensic
8 report in that 2015 Cottom case, right?

9 A. That is correct.

10 Q. And you were one of the investigators. I think
11 there were three or four of y'all?

12 A. There were three of us, yes.

13 Q. Okay. Did the NIT in that case make any fundamental
14 changes to the computers on which it was executed?

15 A. In that case it did not make any fundamental
16 changes.

17 Q. Now, in this case you mentioned something about a
18 fundamental change. What I'm trying to wrap my brain
19 around is what could have been changed fundamentally
20 when there was only a temporary change when the NIT was
21 executed and then it went right back to where it was?

22 A. So by definition, what the NIT is -- what the
23 exploit is going to do is it's going to run code that
24 was not intended to be ran, and that mere fact is that
25 it's altering the system and how it actually works.

1 So again, temporarily that is the case, but
2 there is the possibility that it will modify it
3 permanently.

4 Q. Okay. But then going back to your report in the
5 Cottom case -- I'm on Page 11 here quoting -- you
6 stated -- or the report that you were part of an author
7 of stated the investigators -- which you were one of --
8 do not consider NIT to be hacking in that the NIT
9 exploited a configuration setting that did not require
10 offensive-based actions.

11 Then you end with: Exploitation is not always
12 synonymous with hacking.

13 Do you remember making that statement?

14 A. Yes. Could I clarify?

15 Q. Sure.

16 A. So in that case we didn't really consider what the
17 FBI gave us to be an exploit. We just considered it to
18 be a NIT that was run on the system.

19 So the NIT in that case took advantage of a
20 flaw inside of Flash as opposed to exploiting the system
21 in some way that modifies how the computer ran. So it
22 actually ran as designed; it's just it took an advantage
23 of a proxy setting inside of Flash.

24 Q. Took advantage, exploit, doesn't mean the same thing
25 in computer world?

1 A. No.

2 Q. Okay. That's why I'm an English major. So I'm
3 asking.

4 Let's move on to encryption. In Cottom you
5 testified that the fact that the NIT data stream used a
6 TCP connection was a particular indication of
7 reliability.

8 Do you remember making that statement, or
9 testifying?

10 A. I did, yes.

11 Q. Okay.

12 A. Yeah.

13 Q. And then in your expert report in Cottom, you
14 stated: A TCP connection is a very reliable way of
15 transferring data that provides for ordered data
16 transfer, retransmission, error correction, and flow
17 control.

18 A. Yes.

19 Q. Are you aware that Dr. Soghoian testified earlier in
20 these proceedings that the NIT data stream was
21 unreliable for the mere fact that it wasn't encrypted?

22 A. I was aware that he had testified. I didn't read
23 that portion of the testimony.

24 Q. Okay. Now that I've represented that to you, it
25 doesn't sound like you agree with that necessarily.

1 A. I don't necessarily agree with that statement in
2 that TCP is a fairly reliable method. Again, there are
3 other issues that could be at play when you're talking
4 about just making a TCP connection.

5 There's methods of doing proxies that would
6 make it so that an IP address from one computer would
7 appear to be -- would be used by some other user. So
8 there are other situations where the data acquired from
9 that would not be correct.

10 Q. Okay. But in that report -- again, I'm quoting
11 again: TCP connections are the standard method of data
12 transmission for critical over-the-Internet-based
13 activity such as commerce, authentication, banking, and
14 the transmission of other sensitive information.

15 You said --

16 A. Correct. And I -- also in there we stated there are
17 other possibilities that could have occurred.

18 Q. Okay.

19 A. Other situations that would identify the same user
20 using TCP. So there is TCP and then there is, was it
21 used in a proper manner.

22 Q. Okay. Fair enough.

23 The server component, or data storage
24 component, I don't want to use too many different terms,
25 but you understand what I'm talking about when I say

1 that, right?

2 A. So you're talking about the one that logged the
3 information, the PCAP files, or --

4 Q. The data storage component. The logged data that
5 was captured from the NIT, correct?

6 A. Okay.

7 Q. Follow me. Isn't it true that if you compared the
8 raw network data from the NIT to the data that was
9 provided to defense in discovery and determined that
10 they were identical, then the server storing the data
11 must have stored and reproduced it accurately?

12 A. I don't know if that's necessarily a fair
13 comparison. It was consistent. Again, I'm not running
14 on the exact same IP address. So again, I have no way
15 to verify that.

16 Q. Okay. But if the datasets don't match, then how
17 could the storage component have failed?

18 A. Well, again --

19 Q. I mean --

20 A. If you look at the --

21 Q. I worded that weird. The datasets match. We know
22 that. So how could that component have failed?

23 A. So it could be that that component logged
24 information that was incorrect and it matched some other
25 user's information. I haven't looked at it, so I do not

1 know exactly how it worked.

2 Q. Okay.

3 A. I did say that they are consistent, but I can't
4 verify that it was 100 percent correct.

5 Q. Is it fair to say that the purposes of the tools
6 that the FBI used in this case ultimately was to match a
7 username on the Playpen website to a real person?

8 A. I think to an IP address, if that's correct.

9 Q. Which then you could trace, using subpoenas, to a
10 real person? That's the whole purpose of this?

11 A. Correct.

12 Q. And it sounds like you're aware that in this case,
13 the FBI has alleged the real world identity of
14 "regalbegal" as the defendant, Anthony Allen Jean?

15 A. Correct.

16 Q. And I assume that you're also aware that Mr. Jean
17 confessed to using the moniker "regalbegal" online?

18 A. That was -- that was provided to me at some point,
19 yes.

20 Q. Well, would the fact that Mr. Jean confessed to
21 being regalbegal lead you to opine that the tools used
22 by the FBI in this investigation functioned properly in
23 that they identified Mr. Jean as "regalbegal"?

24 A. I don't know if I could make that conclusion. I
25 know that if that's what he said, then I can't dispute

1 that.

2 Q. Fair enough, Doctor.

3 MR. DEAN: That's all I have, your Honor.

4 THE COURT: Thank you.

5 Anything further, Mr. Alfaro?

6 MR. ALFARO: Just a few questions, if I may.

7 THE COURT: All right.

8 REDIRECT EXAMINATION

9 BY MR. ALFARO:

10 Q. You were asked on cross-examination, Doctor, about
11 the possibility of analyzing the defendant's computer.
12 Is that correct?

13 A. Correct.

14 Q. Are you familiar with what happens to data on a
15 computer over time? Does it become overwritten?

16 A. Yes. So every time your computer reboots, right,
17 it's going to clean up data files. So if there were
18 changes to the computer, eventually they could be
19 corrected or deleted or removed. If you update your
20 operating system, they might be changed. So computers
21 are inherently rewritable and changeable all the time.

22 Q. So it's possible that if sufficient time has passed,
23 anything that was available on a computer, after a
24 passage of time, is no longer there?

25 A. So I would agree that as time passes, you get less

1 and less reliable information and more of it can degrade
2 or be overwritten by your computer, yes.

3 Q. You testified that in the Cottom case, the software
4 that you analyzed didn't make any fundamental changes.

5 A. Correct. I -- in that case, we don't believe that
6 it used what we call an exploit. It was just the NIT
7 payload.

8 Q. Did you know that before you analyzed it?

9 A. No, I did not.

10 MR. ALFARO: No further questions, Judge.

11 THE COURT: All right.

12 EXAMINATION

13 BY THE COURT:

14 Q. Mr. Miller, you have explained that you have, in
15 fact, examined the NIT code and you set up a Linux
16 environment to do an experiment, and you have described
17 the results of your experiment.

18 Based on your analysis of what has been
19 described as the NIT code, do you have any reason to
20 believe that any of that code would have remained on an
21 activating user's computer such as Mr. Jean's computer
22 in this case?

23 A. I would have no idea if it remained or not because
24 the exploit would be the thing that would have removed
25 that after it ran.

1 Q. If you had examined, or if a person had examined
2 Mr. Jean's computer, would that be a way that they could
3 see if the NIT or any remnants of the NIT remained on
4 Mr. Jean's computer?

5 A. I would highly doubt that any remnants of the NIT
6 would be left over on the computer. That would be my
7 best guess.

8 Q. All right. One of the -- well, Mr. Alfaro was
9 asking you some questions about the information that you
10 didn't have and why, as a matter of precaution, it would
11 be helpful to have that information so you could rule
12 out some theoretical possibilities. One of the things
13 that was mentioned is that settings could be changed
14 such that a third party could come in and do nefarious
15 things on the computer. Do you recall that testimony?

16 A. Yes, I do.

17 Q. Were you aware that Agent Alfin has previously
18 testified in this case that the NIT in Mr. Jean's
19 specific situation passed through the locked door of the
20 Tor browser, ran on Jean's computer, and returned the
21 information back to the government server in a matter of
22 approximately 0.27 seconds?

23 A. Yes. I have heard that, yes.

24 Q. If someone was going to do something nefarious to
25 Mr. Jean's computer in terms of taking control over it

1 or downloading some things that he didn't want on his
2 computer, would that have to occur in the 0.27 seconds?

3 A. No. So if somebody was -- if somebody was
4 controlling his computer, they could have done it
5 themselves and he would have maybe not been present,
6 even at the computer, when that occurred.

7 Q. Well, how would the NIT have left that possibility
8 open if it didn't leave any remnants behind on the
9 computer?

10 A. So it's not the NIT that would leave the remnants.
11 It would be the exploit. And if you remember, the
12 exploit is going to run and then it's going to run the
13 NIT, which sends back the information. So the exploit
14 is like your lock pick which you use to open the door
15 and let the NIT in so that it can get this information.

16 Q. So the --

17 A. So --

18 Q. I'm sorry.

19 A. Go ahead.

20 Q. So the third party that would be doing, potentially,
21 these nefarious things to the computer would have to
22 have access to the exploit?

23 A. Yes. And when the FBI was running this, they were
24 actively sending the exploit to all of the users of that
25 website. So anybody on that website would have received

1 at one point a copy of that exploit if they had a copy,
2 they could have leveraged that to do whatever they
3 wanted.

4 So if it was an exploit just for Tor browsers,
5 then they could have attacked anybody that was on the
6 Tor network.

7 Q. And what sort of preparedness would a person have
8 had to have lined up in advance in order to be catching
9 or monitoring or preserving the exploit?

10 A. So they would have to have been proactive and
11 believe that maybe they were being monitored because
12 they were accessing some website that had illegal
13 material.

14 So they would have had to have been active in
15 understanding and advanced. So they would have to, you
16 know, understand how all of this works, how do you
17 capture data streams and how do you get the exploit out
18 of there and use it again.

19 So it would be a fairly sophisticated user in
20 order to do that.

21 Q. Do you consider yourself fairly knowledgeable in the
22 field of malicious and ethical hacking and
23 countermeasures to employ against hacking?

24 A. I do understand how they work, and I have used them,
25 yes. I guess I don't know where your question is

1 leading, but --

2 Q. Well, I guess my question is this theoretical person
3 that potentially could have done something nefarious to
4 Mr. Jean's computer, had they been well prepared and had
5 the sophisticated means, are such people lurking around
6 on the Internet waiting for such opportunities?

7 A. Yes, there are. There are a lot of -- a lot of
8 people and a lot of business reasons why people do --
9 have such techniques for logging this information.

10 If you're trying to protect your corporate
11 assets, we call these people "blue teamers." They are
12 very much trying to monitor their information, monitor
13 what information is going out so that they can defend
14 against people who are attacking.

15 So there are both, you know, people who are
16 hackers, or red teamers, and there's blue teamers. So
17 there's two different groups that, we're always in
18 training, we're always going to conferences, learning
19 the new technique. So there are a fair amount of people
20 that do this, yes.

21 Q. Well, this imaginary person or hypothetical person
22 with nefarious purposes in mind that would have to be,
23 A, sophisticated and, B, set up in advance, would they
24 have to be monitoring the Playpen website at the right
25 precise time or just monitoring the Tor browser in

1 general?

2 A. They could have done either one. Those are definite
3 possibilities. So if they were concerned about their
4 Tor browser doing something, you know, like running this
5 NIT, they could have been proactive and set it up so
6 that they would log this information so they would know
7 what the exploit was, what the payload is.

8 So they could have done some of that in
9 advance; or they could be doing every, you know, Tor
10 website. They could check and see if anything has
11 changed. So it's definitely a possibility. You know, I
12 can't tell what the odds are that somebody would do
13 that, but it's a possibility.

14 Q. All right. Well, one of the questions for the Court
15 is to examine whether this issue that has been raised
16 about the government's lack of providing the exploit
17 code, the Court has to determine, in the legal sense of
18 the word, whether ruling out this potentiality is really
19 a material issue or not.

20 So I am trying to gain some sense for
21 whether what you have described as this sophisticated
22 person that had advance knowledge, that everything lined
23 up and was looking at the right place and the right
24 time, is that something that is probable, likely,
25 possible, or does it fall in a lower end of technically

1 possible but realistically unlikely?

2 A. So I would say that it would be more than very
3 unlikely. It would be above that because a lot of the
4 people who are visiting these type of sites realize that
5 they are a prime target of people like the FBI.

6 So they are very much paranoid in that sense,
7 right, because they understand that they can't do this
8 on the regular Internet. So they do realize that they
9 can't just do it on the regular Internet. They have to
10 go to Tor. And so you're looking at a much more
11 paranoid population than your regular Internet user.

12 Like, somebody who's using Facebook does
13 not care that Facebook is sending back information about
14 them. So it's very much a more sophisticated audience.

15 Q. So they would be -- and I'm exaggerating a little
16 bit here, but just help me understand. Would it be a
17 situation where such a user would be -- perhaps have
18 more than one screen, and on one screen, they're viewing
19 or accessing website content, and then on another screen
20 view it in a programmer -- view that same content but in
21 a programmer's type language?

22 A. Yeah. So you could be viewing -- you could be
23 viewing the actual page and then you can have software
24 that's running in the background that would log all of
25 the information that's going on, see if the page has

1 changed from the last time that you viewed it in some
2 substantial way.

3 So that is definitely something that people do.
4 People do use that type of software and develop that
5 type of software.

6 Q. And there are obviously, as you described, blue
7 teams in all different sorts of corporate environments.
8 In any of the cases that you have been associated with
9 as a consultant, have you ever run across some third
10 party who was capturing this software in the background
11 for the very purpose of being in a position to do
12 something nefarious with it after the fact?

13 A. Yes. People do do that. They will look at --
14 especially people who are trying to defend networks.
15 They won't use it maliciously, but they will capture
16 that information. And the mere fact that they captured
17 it, they would have the ability to use it if they so
18 desired.

19 So that's what a lot of corporations are trying
20 to do is trying to figure out what -- which of their
21 computer systems have been compromised and so they use
22 software that logs that information. And that type of
23 software is available for people to use.

24 Q. All right. If I can paraphrase your earlier
25 testimony, you've said that you wouldn't rank it as

1 something that was likely to have happened but probably
2 somewhere above very unlikely to have happened.

3 If you take the starting point as something
4 that is very, just a little -- or at some point above
5 very unlikely to have happened and you put that into the
6 context of the government's contention here that
7 Mr. Jean has admitted that he used the regalbegal avatar
8 and has admitted that he downloaded child pornography
9 from the Playpen website, what does that do to your
10 relatively -- relativity scale of some third party
11 obtaining this code and surreptitiously getting on
12 Mr. Jean's computer and putting other material there?

13 A. Given that evidence, I would say it's much less
14 likely.

15 Q. All right. Now, the Cottom case that you have
16 talked about, my understanding from what I could gather
17 in looking at that docket in that case is that the
18 defendant's position and the theory of the defense in
19 that case was that there was no evidence that Cottom had
20 made any effort to download any specific image from the
21 website in question. Is that correct?

22 A. I believe so, yes.

23 Q. And I believe it was also the defense position, if
24 I'm understanding it correctly -- and you correct me if
25 you recall otherwise -- but my understanding is that the

1 defense took the position that there were not any images
2 on his computer that originated from the website in
3 question in that case. Is that correct?

4 A. I don't recall the specifics on that part. Again, I
5 didn't -- I don't really do sort of computer analysis
6 but, you know, I know they had found files in sort of
7 what we call slack space or where -- you know, where the
8 computer says it's going to delete something but then it
9 just sort of marks it with an X saying it's going to
10 delete it later. So I would have to -- I would have to
11 look again. That wasn't my part of the analysis that I
12 did.

13 Q. On the unique identifier, to the extent that the
14 government is accurate in stating that Mr. Jean has
15 admitted to using the regalbegal avatar and has admitted
16 to downloading images from the Playpen website, how
17 would you characterize the materiality of needing to
18 know how the algorithm was coded to generate a unique
19 identifier number?

20 A. So my guess would be the only -- I'm given that that
21 additional evidence, the benefit of having it would be
22 to know whether or not that number, which was four, was
23 high or low. Did it accidentally log it four times
24 because of something or did it not log it -- you know,
25 it was supposed to be ten and it only did four.

1 So that would be the extent of what we could
2 say on that end.

3 Q. All right. I believe you said that you have read
4 Agent Alfin's affidavits in other cases; is that right?

5 A. Yes, that is correct.

6 Q. Do I recall correctly that he has testified by
7 affidavit in other cases that he's conducted an analysis
8 of matching up the unique identifiers that were
9 originated and being able to match all of those up with
10 the information that came back from the activating
11 computers?

12 A. Yes, I believe that's what he's testifying.

13 Q. To the extent that that is accurate or credible,
14 what impact does that have on this theoretical
15 possibility that you have explained about the
16 identifiers?

17 A. I don't -- I don't know if it necessarily changes
18 that. Again, we haven't had to -- we haven't looked at
19 it to see are there possible errors in the code that
20 generated it. So...

21 MR. DEAN: I think we just lost him.

22 CLERK CRAIG: Tyler?

23 (Short interruption of proceedings.)

24 THE COURT: Sorry about that, Mr. Miller.

25 THE WITNESS: That's all right.

1 Q. You said that you were provided with the NIT code in
2 this case, which, I understand that the term "payload
3 code" would be synonymous with the term of how I've
4 described the term "NIT code." Is that right?

5 A. That is correct.

6 Q. And that was provided to you in a binary format?

7 A. Yes.

8 Q. And you were saying that it would be -- have been
9 more helpful to you if it was provided in a more
10 reader-friendly version? Is that right?

11 A. That is correct.

12 Q. What would be the name of a more reader-friendly
13 version that you believe the FBI -- or the government
14 would be capable of producing it in?

15 A. So generally when you -- the human-readable version
16 of it is called source code and then when you use what
17 we call compiler, you generate the binary code that
18 would be sent and run.

19 Q. Is the term "source code," is that a language, or is
20 that a descriptive term of just the human-readable form?

21 A. So it's the descriptive term. There are lots of
22 different languages you could write it in. We have Java
23 and C. There's a lot of different languages we could
24 write it in as humans, but if it's going to get run on
25 the computer, it has to be converted from that human

1 language into the computer language and that's the
2 binary code.

3 Q. All right. So given that, what is your criticism of
4 being provided the binary code as opposed to more --
5 some more human-readable format?

6 A. Well, partially because it makes it much more
7 difficult to read because when you take that binary code
8 and you bring it up one level to something that's
9 human-readable, it's much more difficult to read.

10 So, for example, if we look at the report that
11 I gave -- and I don't know if you have a copy of it, but
12 in part of their -- of the NIT, there was actual
13 human-readable code. There were what we call comments
14 which describe what it's going to do, and it helps to
15 verify that something -- when you're writing code, you
16 put in comments so you know what it's doing.

17 And so my criticism would be that they weren't
18 providing us with the actual source code. They were
19 just providing us with the binary code. And again, it
20 makes my job much more difficult. It takes longer to do
21 it.

22 And there are possibilities that I could miss
23 something or that something in the source code, you
24 know, maybe it had a specific condition that it
25 generated different source code. I wouldn't be able to

1 see that if I don't have the original source code that
2 was used to generate that.

3 Q. Well, which language, programming language, are you
4 most familiar with that would -- that you think that the
5 government could reasonably provide -- what language
6 could they reasonably provide source code in that you
7 would be most familiar with?

8 A. I would be familiar with whatever they provided. I
9 don't know what they used. They could have used
10 assembly or they could have probably used C, which are
11 two different languages, but again, I don't have -- I
12 don't know what they use, but whatever I would be given,
13 I would be able to analyze because most programming
14 languages that are human-readable are fairly easy to
15 pick up when you know one of them and just learn another
16 one really quickly. But I'm familiar with a lot of
17 different languages.

18 Q. Are there not any -- is there not any software that
19 takes the binary code and translates it back to a
20 programming language, a source code language?

21 A. So can I -- this might be a little bit complicated,
22 but if you start with, I said C.

23 Q. Yeah.

24 A. And so C you're going to generate an assembly, which
25 is a lower level than C and then you're going to

1 generate binary. In this process, you lose information.

2 So information like comments go away.

3 Information about labels, about different conditions

4 that generate different code will all go away and so

5 when you pull it back up one level, you're only going

6 one level, not clear to the source code. So there's

7 information that's inherently lost in doing this.

8 And, yes, I do have a program that does it, and

9 I brought it up and I've analyzed, you know, four or

10 five of these and so I'm getting fairly good at reading

11 it, but again, it didn't feel like a good faith effort

12 for them to not provide us with the actual source code.

13 Q. You mention that you were retained in some of the

14 other cases that originated -- or that evolved out of

15 the Playpen criminal litigation. I believe Michaud and

16 Matish?

17 A. Matish, yes.

18 Q. Matish? Did you run the NIT code on either of the

19 subject computers in either of those cases?

20 A. So I did not get the code in Michaud. In Matish I

21 was given the code. And I didn't run it on their

22 computer; I ran it in my test environment. And again, I

23 got similar data in those cases. It was consistent with

24 the PCAP -- or the data stream that was provided.

25 Q. All right.

1 THE COURT: Mr. Alfaro, does that prompt
2 anything further?

3 MR. ALFARO: It does, your Honor.

4 REDIRECT-EXAMINATION

5 BY MR. ALFARO:

6 Q. Dr. Miller, the Court asked you about these people
7 that may have nefarious purposes, that were monitoring
8 these type of websites. Do you remember that?

9 A. Yes.

10 Q. Are you familiar with such a thing happening in 2013
11 when someone actually caught the exploit?

12 A. I don't recall that case, but I'm -- if you have
13 one, I'm sure that it references what you said.

14 Q. Does it sound familiar, the Tor Mail case?

15 A. Yes, I do recall seeing some NIT source code that
16 was released for a different NIT that was deployed. So
17 I have seen that one.

18 Q. So in the past there's actually been someone that's
19 got --

20 MR. DEAN: Objection. I don't see how this is
21 relevant. He said it was a different source code. He
22 wasn't even familiar with it until he led him do it. I
23 just, I don't really want --

24 THE COURT: Well, the Court opened the door to
25 whether this stuff is actually going on. So I think

1 that's a fair followup.

2 MR. ALFARO: Yes, Judge.

3 Q. So in that Tor Mail case, there was actually someone
4 monitoring the exploit and they caught it?

5 A. Correct.

6 Q. In your opinion would it be helpful for the defense
7 to have a copy of the source code?

8 A. Yes, it would.

9 Q. Would it be helpful for the defense to have a copy
10 of the source code for the exploit? Clarify that
11 question.

12 A. So for the exploit, I don't necessarily know if
13 there would be source code for the exploit. A lot of
14 times exploits are written in such a way that you don't
15 generate -- you don't have source code in order to
16 generate them. So I don't even know if that exists or
17 not.

18 Q. Would it be helpful for the defense to analyze what
19 we are referring to as the exploit in any language?

20 A. Yes. So if we were given the binary exploit, we
21 would be able to -- I would be able to reverse engineer
22 it up to that assembly level, and I'd be able to do some
23 analysis on it just like I did with the NIT that was
24 provided.

25 Q. Would it be helpful for the defense to review the

1 server component aspect we discussed?

2 A. Yes. If we were able to review it as I did in
3 Cotton, we would be able to verify that it generated the
4 correct unique identifiers and that it logged that
5 information in a proper format that wasn't -- couldn't
6 be modified after the fact and things like that.

7 Q. And the same for the unique identifiers?

8 A. Yep.

9 MR. ALFARO: That's all I have.

10 THE COURT: Mr. Dean?

11 MR. DEAN: I don't have anything further, your
12 Honor.

13 THE COURT: All right. Mr. Alfaro, may
14 Mr. Miller be excused, or would you like him to
15 participate via video or standby via video?

16 MR. ALFARO: Judge, if it's all right with the
17 Court, I would like him to remain and listen via video
18 in case I need to call him via rebuttal witness.

19 THE COURT: All right. That's fine. Any other
20 witnesses, Mr. Alfaro?

21 MR. ALFARO: No other witnesses, your Honor.

22 THE COURT: All right. Mr. Dean, you may
23 proceed.

24 MR. DEAN: I'll call Special Agent Daniel
25 Alfin.

1 THE COURT: Agent Alfin, if you'd please
2 approach the bench and raise your right hand.

3 DANIEL ALFIN,
4 having been first duly sworn, testified as follows:

5 THE COURT: You may inquire.

6 MR. DEAN: Thank your Honor.

7 DIRECT EXAMINATION

8 BY MR. DEAN:

9 Q. Please reintroduce yourself to the Court.

10 A. Good afternoon. My name is Daniel Alfin, last name
11 spelled A-l-f-i-n. I am a special agent with the FBI.
12 I am currently assigned to FBI headquarters, Criminal
13 Investigative Division, Violent Crimes Against Children
14 section, Major Case Coordination unit, located in
15 Maryland.

16 Q. And how long have you been employed by the Federal
17 Bureau of Investigation?

18 A. I have been a special agent with the FBI since 2009.

19 Q. And are you the case agent for the national Playpen
20 investigation that's at issue in this case?

21 A. I am.

22 Q. And in fact, you previously testified in this Court,
23 I believe it was back in May, regarding a hearing on
24 defendant's motion to suppress?

25 A. Yes, I did.

1 Q. Have you reviewed that testimony that you gave
2 previously to the Court back in May?

3 A. I have. I have read the transcript of that hearing.

4 Q. Is there anything that, after reading that
5 transcript, you feel you need to address or correct?

6 A. There is. There was a small misstatement in my
7 testimony. I wasn't sure after the fact if I had
8 misspoken or if I didn't speak clearly into the
9 microphone, but on one page of the transcript, I am
10 quoted as saying that the Tor network is comprised of
11 hundreds of thousands of computers. I meant to say
12 hundreds or thousands of computers.

13 I believe the Tor network currently stands
14 somewhere between 7- and 8,000 nodes around the world,
15 not hundreds of thousands. If I did misstate that, that
16 was not intentional.

17 Q. Is that a real important issue in that suppression
18 hearing?

19 A. It is not, but I wanted to correct my testimony, as
20 it was not factually accurate as it was written.

21 Q. Okay. And you want to perfect your testimony
22 because, are you testifying in other courts around the
23 country?

24 A. I am testifying in numerous cases.

25 Q. All right. Thank you, Agent Alfin.

1 Moving on to the current issue and that's the
2 motion to compel, did you author a declaration
3 pertaining to this matter in United States versus
4 Matish?

5 A. I did.

6 Q. Please describe for the Court what information and
7 evidence has been provided to the defendant, Anthony
8 Jean, regarding this case.

9 A. In the matter at hand, the defendant has been
10 provided with what has been referred to thus far by the
11 government as the NIT. It has also been referred to as
12 the payload.

13 This piece of evidence is all that would be
14 needed in order to verify that the government did not
15 exceed the scope of the -- what has been referred to as
16 the NIT warrant.

17 Importantly the payload that was provided, the
18 binary file that Dr. Miller analyzed, it can be executed
19 and tested as I have done, as Dr. Miller has also done,
20 and its output can be observed.

21 So if you were to run this, the payload, on a
22 computer, you would actually see it reach out to the
23 Internet and send the items that the NIT warrant
24 authorized it to collect to the IP address of the
25 government server. You would also see that contained in

1 that data stream is nothing other than what was
2 authorized by the NIT warrant.

3 In addition to that, it is worth noting that we
4 turned over the two-way data stream that resulted as a
5 result of the execution of the NIT on Mr. Jean's
6 computer, and what's important in this is that it is a
7 two-way data stream.

8 So you can see both ends of the communication.
9 Mr. Jean's computer reaches out to the government
10 server, it acknowledges that connection, data is
11 exchanged, and the connection is closed.

12 You can see that the -- that Mr. Jean's
13 computer sent the information that it was authorized to
14 collect to the government server, and you can see that
15 in response to that, the government server did not send
16 images of child pornography back to his computer. It
17 didn't respond and send any additional instructions to
18 his computer.

19 After Mr. Jean's computer sent the information,
20 the connection was closed. As previously noted by the
21 Court, that communication took approximately .27
22 seconds.

23 And so these two pieces of information can be
24 used to verify everything that the defense would need in
25 order to verify that the tools used by the government

1 functioned as intended and that they did not exceed the
2 scope of the search warrant. Again, they can be tested,
3 they can be analyzed, their output can be observed, and
4 they can be compared to what was collected by the
5 government in Mr. Jean's case to confirm that the tools
6 worked as intended.

7 The other significance of the PCAP data, the
8 two-way network data stream, is that what we collected
9 and what we provided to Dr. Miller for analysis is the
10 actual raw data that the government collected. This is
11 as it came into the government server before it touched
12 any server components, before it got into what's been
13 referred to as a network component or a server storage
14 component. This was the actual raw data.

15 And so you can take this actual raw data, and
16 you can compare it to what was provided to Mr. Jean in a
17 report that he was given. You can see that the report
18 accurately reflects the raw data that was collected.

19 Comparing these two datasets, assuming that
20 they match -- and they do match in this case -- there is
21 no way that the data storage component could have failed
22 because we know that before -- we had the data before it
23 even hit this data storage component and so if the data
24 matches on the front end to the data that was provided
25 on the back end, there is no -- there is no possibility

1 that the data was stored improperly. It matches on both
2 ends; so it was clearly not tampered with, intentionally
3 or unintentionally, while it was on any government
4 server in storage.

5 Q. And those are the two main components that have been
6 turned over to the defendant?

7 A. Correct.

8 Q. What has not been turned over to the defendant in
9 this case that, by the testimony and statements made
10 here today, you think they're requesting?

11 A. The Court, in opening, I believe clearly laid out
12 the requests that defense has made, and those -- and the
13 Court's understanding is accurate.

14 The one item that the defense is requesting is
15 the exploit that was used in this case, and as the Court
16 accurately described, the exploit could be thought of as
17 tools and methods that allow for the execution of the
18 NIT, the NIT being what actually collects data and sends
19 it back to the government. That exploit has not been
20 turned over to defense. The government has maintained
21 the position that it is not material.

22 Another item that has not been turned over to
23 defense or described to defense is the methodology by
24 which unique identifiers were generated in this case.
25 That information has also not been provided.

1 On the matter of the unique identifiers,
2 Dr. Miller in his testimony earlier today, misstated the
3 purpose of the unique identifier. I don't believe that
4 this was an intentional misstatement, but to clarify,
5 the unique identifiers that were generated, their
6 purpose was not to track user activity on the website.
7 They were not stored and then later correlated to future
8 logins should regalbegal come back, I believe it was
9 four times.

10 That unique identifier that was used as part of
11 the NIT was not responsible for tracking user activity
12 on the website or correlating different login sessions.
13 The purpose of the unique identifier, when it was
14 generated, it was injected into the NIT and it was sent
15 along with the data being used by the user, in this case
16 regalbegal. And when that unique identifier comes back
17 in NIT results, we can match it up and say this unique
18 identifier went to regalbegal, this is the IP address
19 that it came from, so this is the IP address that we are
20 alleging is associated with regalbegal.

21 Again, the unique identifier does not track
22 user activity on the website or correlate various login
23 sessions.

24 Q. So the unique identifier was a one-time thing during
25 that .27 seconds when the NIT was going back and forth?

1 A. Correct. I believe what Dr. Miller was associating
2 the unique identifier with on message boards is commonly
3 referred to as a session ID or a session identifier.
4 Separate issue from the unique identifiers that were
5 part of the NIT.

6 Q. So the statement for four times on the website, high
7 or low, that means nothing with the unique identifier?

8 A. Correct. That is -- that is a completely separate
9 issue.

10 Q. Now, you've mentioned two things that the defense
11 seems to want that the government hasn't turned over,
12 but we heard about a third one. What about this issue
13 of the code used to create the NIT that they are asking
14 for?

15 A. The -- so it became, I believe, more clear to me
16 early today, recently hearing Dr. Miller testify. And
17 so what has been turned over is the binary code and an
18 assembly representation of that code. Assembly language
19 is commonly referred to as a low-level programming
20 language.

21 Typically, as Dr. Miller testified to
22 accurately, programming code is written in higher level
23 languages. A number that Dr. Miller noted were I
24 believe C, Java, and he may have mentioned some other
25 ones. And so those are languages that are easy to look

1 at and easy to read and code in.

2 And so at a certain point in the process of
3 compiling code, you end up with assembly code, which is
4 not user-friendly. It's not easy to look at and
5 immediately know what it does. And so I believe the
6 assumption has been to this point that the NIT was
7 originally written in one of these higher level,
8 user-friendly codes.

9 That is not the case. The NIT that was used in
10 this case was actually written in assembly language, and
11 assembly language does have an either one-to-one or near
12 one-to-one relationship with the actual binary code that
13 is being run. And so if a program was written in
14 assembly language, then looking at the material that we
15 provided, you can accurately come to conclusions about
16 what the code does and does not do.

17 Q. So as far as that request, it is what it is, and
18 anything else doesn't exist?

19 A. Correct. There is no high-level source code. I
20 believe that's what defense was requesting.

21 Q. Could turning over the unique identifier generator
22 or the exploit, in your opinion, aid the defense in any
23 way?

24 A. No.

25 Q. Explain your basis for that opinion.

1 A. I've provided previous testimony, and it's also
2 referenced in my affidavit. First, with the exploit.
3 Looking at the exploit -- and again, the exploit is what
4 enabled us to run the NIT on the computer. I believe
5 Dr. Miller's description of this in his testimony was
6 accurate in as much as what the exploit allowed us to do
7 in this case.

8 Comparing that to making entry into a physical
9 house when you execute a search warrant, if you use a
10 lock pick to enter a house, you can look at the lock
11 pick as long as you want. It's never going to tell you
12 what agents did after they entered the house.

13 A lock pick doesn't seize evidence. It doesn't
14 do anything material. After the lock pick serves its
15 purpose, agents go into the house, they seize items,
16 they take pictures. And so if you want to know what was
17 actually done on the defendant's computer, we provided
18 the defense everything that they need to do that.

19 We provided them with the NIT. It can be
20 tested. I have tested it. Dr. Miller has tested it,
21 and I believe Dr. Miller also testified earlier that the
22 output that he observed did appear to match what the
23 government has provided in discovery that we have
24 alleged has come from Mr. Jean's computer.

25 And so looking at the exploit has no bearing on

1 any of the actual evidence in this case. The same thing
2 applies to the software used to generate and inject a
3 unique identifier. I have looked at all the unique
4 identifiers generated in this case. They are, in fact,
5 unique. Generating unique identifiers is not a
6 difficult process. There are numbers of programming,
7 software functions and libraries that serve this
8 purpose. It is not a difficult thing to do. More
9 importantly, in this case it was done properly. They
10 were all unique.

11 And I'll go a step further and say that for the
12 sake of argument, had there been some failure, had they
13 not been unique, it would still have no bearing on this
14 matter because, again, the purpose of all the tools used
15 in this case was to associate a member on the Playpen
16 website with a person in the real world, and we did that
17 in this case.

18 That individual, Mr. Jean, confessed to what we
19 alleged he did and so even if there was some glitch, a
20 unique number was generated more than once, it would
21 still have no bearing on the matter at hand. Unique
22 identifiers were, in fact, unique in this case. So it's
23 a nonissue. However, any alleged glitch in that
24 software would still have no bearing on this matter.

25 Q. Agent Alfin, are you familiar with Dr. Miller's

1 expert report that he issued in the Cottom case?

2 A. Yes. I've read it.

3 Q. And he said in that case the exploit -- he didn't
4 refer to it as an exploit. He referred to it as
5 something that enables you to get to -- I mean, he
6 basically said "exploit" without saying "exploit" as a
7 synonym. But what is the difference between the
8 exploit-type piece of software that was used in the
9 Cottom case and the one involving this case that we have
10 not turned over at all?

11 A. Well, first of all, the Cottom report does actually
12 say "exploit." So it does go into -- in the page of the
13 report describing that function, it does actually use
14 the word "exploit."

15 I know Dr. Miller testified earlier that -- I
16 believe he said that his -- he and his colleagues did
17 not necessarily consider the NIT in that case or,
18 rather, there to be any exploit in that case, but the
19 report does say "exploit." And so Dr. Miller also
20 testified that the government turned over everything, or
21 almost everything, that the defense experts had
22 requested in that case.

23 I will -- I think it's important to note in
24 that case the government did not concede materiality for
25 the items that were turned over, but they were turned

1 over for that analysis.

2 Q. What was the -- then if we're calling them both
3 exploits, was there a difference in the exploit in
4 Cottom and the one involving Mr. Jean, and if so, what
5 is the difference in that exploit? Why was it turned
6 over in one and not in this one?

7 A. So again, we did not concede materiality in the
8 Cottom case. However, there was -- there was nothing
9 sensitive in the -- in the Cottom case. It was a
10 well-known published exploit that I believe at the time
11 of the analysis was no longer viable. It didn't work
12 anymore.

13 The Tor browser now has protections against
14 that sort of thing. I believe it had protections
15 against that sort of thing at the time, but they have
16 since been made much stronger. And so, again, we did
17 not concede materiality in that case, but there was --
18 there was nothing sensitive about any of the tools or
19 technologies used in that case.

20 Q. Fair to say that Cottom involved off-the-shelf
21 technology and Jean -- Playpen -- involved
22 still-sensitive technology that can be used?

23 A. There is law enforcement-sensitive material involved
24 in the Playpen matter and that was not the case at the
25 time of the analysis in the Cottom case.

1 Q. You were present for Dr. Miller's testimony,
2 correct?

3 A. I was.

4 Q. When we got into the -- or he got into the
5 discussion about blue teamers able to possibly hack
6 Playpen, do you agree with his analysis about the
7 sophistication that a hacker would have to have? Just
8 that whole line of testimony, what is your opinion on
9 that?

10 A. So in order for a -- someone to have captured the
11 FBI's exploit in this case, that individual, first of
12 all, would have had to have been an active member of the
13 Playpen website. There was not an exploit or an
14 operation where we were just blasting things out to
15 every user of the Tor network. This was specific to the
16 Playpen website.

17 And so, first of all, in order for someone to
18 have captured the FBI's exploit, they would have had to
19 be a member of the Playpen website, and they also would
20 have had to be doing a number of things.

21 First of all, they would have to have been --
22 well, aware of the FBI's operation in order to know to
23 even look for such an exploit. But second of all, they
24 would have had to have the capability and software
25 configured on their computer to intercept traffic

1 between the Tor proxy on their computer, or traffic
2 going into and out of the Tor proxy on their computer.

3 I've testified, I believe last time in the
4 previous hearing, that data going over the Tor network
5 is encrypted. With Tor hidden services, such as the
6 case with the Playpen website, that is end-to-end
7 encryption. So the data is encrypted at your computer,
8 and it is encrypted at the destination server.

9 So, first of all, that precludes someone who
10 knows about the Playpen website from just, even if they
11 know where it is, from monitoring activity going to and
12 from that Playpen website. That data is all encrypted;
13 it would do them no good. So they are not able to get
14 the exploit there, if they even know about the
15 operation.

16 Now going back to what it would take for a
17 member of the Playpen website to have captured the
18 exploit, they have to be monitoring traffic on their
19 local computer, going to and from the Tor proxy on their
20 computer.

21 When you are connecting the websites, in this
22 case downloading child pornography through the Tor
23 network, that is a massive amount of data to go through.
24 And in order to realistically find that exploit, you
25 would likely need to have firsthand knowledge of it on

1 the front end. You'd have to know what you're looking
2 for really.

3 The odds of someone, A, knowing about the FBI's
4 operation, knowing that we were using this exploit and
5 then having the tools and capabilities to capture and
6 analyze all the data going to and from the Tor proxy and
7 their computer and then actually finding that exploit in
8 a format that they could actually reuse it for their own
9 purposes I would say is zero, whatever tiny number is
10 slightly higher than zero.

11 It is a farfetched theoretical possibility.
12 There is no evidence to suggest that anything like that
13 occurred in this case at all.

14 I would also note that in the description that
15 was given for, I believe defense referred to it as the
16 Tor Mail case, that was a completely separate operation
17 with separate tools and techniques used in that case, a
18 significant difference being from the two cases: There
19 were legitimate uses of some of the websites that were
20 hosted on the servers that had been taken over by the
21 government.

22 Tor Mail itself was not illegal. It was
23 certainly frequently used for illegal purposes, but you
24 could have a Tor Mail account; you could use the
25 Tor Mail website without committing a crime, so the odds

1 of someone, you know, finding an exploit there.

2 I would also note that the exploit was deployed
3 in that case in a much different manner than in Playpen.
4 So there was no one-to-one comparison that could be
5 drawn but someone could legitimately, a security
6 researcher could go to a website like Tor Mail, if it
7 hadn't been compromised, and look for anomalies, look
8 for exploits, things of that nature.

9 The Playpen website did not have legal
10 functions. It was a child pornography website. So
11 again, the odds of someone actually finding and
12 utilizing the exploit that was deployed in this case for
13 the approximately 13 or 14 days that the FBI had control
14 of the Playpen website is next to zero.

15 Q. Thank you.

16 MR. DEAN: Your Honor, that's all I have.

17 THE COURT: Thank you.

18 Mr. Alfaro?

19 MR. ALFARO: Yes.

20 CROSS-EXAMINATION

21 BY MR. ALFARO:

22 Q. Agent Alfin, the fact that a website is legal or
23 illegal changes your analysis of how someone can capture
24 an exploit?

25 A. Certainly.

1 Q. Why is that?

2 A. Well, as I said, on a legal website, you're likely
3 to have security researchers. You're likely to have
4 people, more people with significant technical expertise
5 who can do these types of things, who maybe -- may be
6 looking for that type of stuff.

7 Q. So you're --

8 A. You're not going to find -- can I finish answering?

9 Q. Yes, sir.

10 A. You're not going to find a user base on a website
11 whose purpose is illegal. There's no security
12 researcher exemption for becoming a member of a child
13 pornography website.

14 Q. So is it your opinion that the majority of the users
15 of Playpen were not sophisticated?

16 A. Sophisticated in what manner?

17 Q. Had the sophisticated expertise or ability to do
18 something like what happened in Tor Mail case versus the
19 Playpen case?

20 A. I would say based on my training and experience and
21 being familiar with the various Playpen cases, the
22 majority of users on the Playpen website that I'm aware
23 of would likely not have the expertise to capture an
24 exploit in the wild and retool it for their own
25 purposes.

1 Q. How many people is that?

2 A. How many people is what?

3 Q. The people that you're familiar with that don't have
4 the expertise.

5 A. I believe it's the approximately 200 or so people
6 that have been arrested. That's a public stat. I don't
7 know if it was released in this case or a separate one,
8 but I think that's still relatively accurate.

9 Q. How many people -- how many times was a NIT
10 deployed?

11 A. Against Mr. Jean? Once.

12 Q. How many times was a NIT deployed in your operation
13 of Playpen?

14 MR. DEAN: Objection. I think we got into this
15 in the suppression hearing, your Honor, and I don't
16 think it was relevant then; I don't think it's relevant
17 now.

18 THE COURT: Mr. Alfaro?

19 MR. ALFARO: I think it's relevant now if Agent
20 Alfin is representing the majority of the people don't
21 have the capacity to do what is possible in regards of
22 getting this exploit. If he's analyzed 200 people,
23 okay, out of how many? 200 out of 250? That lends
24 credibility to his testimony. 200 out of 100,000 people
25 or more, I think that calls into question his statement.

1 Moreover, I think the higher the number, the
2 more risk that is present in someone capturing this. So
3 I think that information is extremely relevant.

4 THE COURT: Well, I get your argument. You can
5 certainly -- that's kind of commonsensical and I can
6 certainly appreciate that argument but I don't know that
7 for purposes --

8 MR. ALFARO: Judge, I apologize. I can't hear
9 very well.

10 THE COURT: I said that I can appreciate the
11 commonsense nature of that argument in the sense that if
12 they have arrested 200 people and they believe that it
13 was deployed more than that, then they don't have
14 everyone that may have accessed the site and, therefore,
15 they don't have a way of measuring their level of
16 sophistication.

17 I think you're trying to squeeze out the Nth
18 degree of some point that is not really necessary and
19 would justify going down that path for the reasons that
20 we explained last time that we were here. So I'm going
21 to sustain the objection.

22 MR. ALFARO: Thank your Honor.

23 Q. Agent Alfin, did you write the code that generated
24 the unique identifier?

25 A. No, I did not.

1 Q. Did you write the code for the exploit in this case?

2 A. No, I did not.

3 Q. In your affidavit, do you generally agree that it's
4 possible for an exploit to make a fundamental change or
5 alteration to a computer system or disable a security
6 firewall?

7 A. I believe that is a quote -- or a paraphrase from my
8 declaration. Some exploits can do those things, yes.

9 Q. Did you write the unique -- I'm sorry. Did you
10 write the code for the server component?

11 A. No.

12 MR. ALFARO: Judge, if I may have a -- if this
13 is an okay time, may I have a minute for a brief recess
14 to consult with Dr. Miller?

15 THE COURT: You may.

16 We will be in recess for 15 minutes.

17 (Recess from 4:25 p.m. to 4:39 p.m.)

18 THE COURT: Mr. Alfaro, I believe it's your
19 turn. Do you have any more questions?

20 MR. ALFARO: I do have just a few, your Honor.

21 Q. Agent Alfin, to your memory, was the NIT ran on
22 Mr. Jean's computer in March of 2015?

23 A. If that's what the -- that sounds accurate. I don't
24 remember the exact date, but that is during the
25 timeframe of our operation. If that's what the report

1 you have says, then I believe that's accurate.

2 Q. Would that be accurate to you, the best of your
3 recollection, that his computer was seized on July 9th,
4 2015?

5 A. I don't know the exact date it was seized, but
6 again, it sounds accurate.

7 Q. Agent Alfin, I believe in your declaration,
8 referring to the exploit, you said that you've ran the
9 exploit and reviewed the computer settings; is that
10 correct?

11 A. On the computer on which it was run, yes.

12 Q. What security settings did you test?

13 A. So, first of all, the computer that I was running
14 was a virtual machine. It was also running a Linux
15 operating system similar to what Mr. Jean was running
16 and so first thing that I tested was running a command
17 on the system to see active networking connections.

18 And so a common test that an individual
19 performs when analyzing a computer for signs of malware
20 infection or things of that nature are looking at active
21 network connections. And so if you run a piece of
22 software that you think may be having some unintended
23 side effects, you would look at the active network
24 connecting, software, and then see if there are any
25 other active connections. That was one of the things I

1 did.

2 The other settings that I looked for were
3 basic, and the operating system was Linux Mint, which is
4 a variant -- or I believe it's based on Ubuntu Linux,
5 which is what the defendant was running.

6 And so there are built-in defaults, settings
7 files on the computer. In the directory, the directory
8 structure I don't remember off the top of my head. I'm
9 not going to be able to remember specific filenames, but
10 certain things like what services are configured to run
11 upon boot-up, I believe those are in a file directory
12 named RC.D, and there are various other RC.D directories
13 as well with various numbers after them. And so you can
14 see in there to see if, you know, programs are booting
15 up that you don't expect.

16 You can also look and, depending on what
17 firewall you are using on the computer installation, you
18 can see if there are any changes in there that are not
19 changes as a result of software that you had intended to
20 install on the computer or the default configurations
21 for those, for those files.

22 And so I looked at a handful of those
23 configuration files. They appeared to be either in
24 their default configuration or had configurations in
25 them that were the result of software installed on a

1 machine. So intended changes.

2 I did not see, in any files that I analyzed or
3 any of the active network connections, anything
4 unintentional. There was no -- most importantly, with
5 this type of software, one of the things that's been
6 alleged is that maybe it left the computer vulnerable to
7 outside intrusion and so if your computer is vulnerable
8 to outside intrusion frequently, it will be, we say
9 listening on a particular port on the computer.

10 Ports are tied to IP addresses and they will
11 allow you to connect out of your computer and allow
12 other people to connect into your computer. And so
13 looking at those active ports is really one of the most
14 important things to know whether or not your computer
15 has been left in a state that would make it vulnerable
16 to outside intrusion, and again, I did not notice any --
17 any changes or any unintended services on the computer
18 listening for such connections.

19 Q. Did you review every single security feature?

20 A. I did not review every single file on the computer.

21 Q. Would you agree that it's possible for there to be
22 unintended consequences through human error when
23 preparing and using things like an exploit code?

24 A. Separate from this investigation, other exploits,
25 yes, things can go wrong and there can be unintended

1 consequences.

2 Q. I believe you testified that the unique identifier,
3 when it's generated, it needs to be logged and saved on
4 the computer; is that correct?

5 A. On the government server, or the user's computer?

6 Q. Either.

7 A. Well, we don't save anything on the user's computer.
8 Nothing, nothing remains behind. So the unique
9 identifier is not saved on the user's computer.

10 Q. Did you look at the code that stored the unique
11 identifier?

12 A. Sir, can you clarify the question?

13 Q. Did you look at the code that stored the unique
14 identifier on the government server?

15 A. That's the same question. But are you referring to
16 what you previously described as the server component?

17 Q. Well, I guess let me see if I can clarify. Would
18 you agree that the unique identifier needs to be stored
19 on the government computer?

20 A. Yes, it does need to be stored.

21 Q. In order for it to be stored, there has to be a
22 process to create a method for storing it. Is that
23 correct?

24 A. Generally, yes.

25 Q. Were you part of that process?

1 A. No, I was not.

2 Q. Is there a code that's generated to -- that's used
3 to capture the information that's displayed in the PCAP
4 file?

5 A. I'm sorry. Can you clarify that question, please?

6 Q. The PCAP file that's generated, it -- again, I think
7 your testimony was that it monitors what is sent and
8 what is received from the NIT. Is that correct?

9 A. So --

10 Q. It's a two-way network?

11 A. So the PCAP data is the actual data that was
12 received by the government. It is not a program. The
13 PCAP data is the raw data that was received from the
14 government as the result of the NIT's execution on
15 Mr. Jean's computer.

16 MR. ALFARO: That's all I have, your Honor.

17 THE COURT: All right.

18 Does that prompt anything further?

19 MR. DEAN: It does not, your Honor.

20 EXAMINATION

21 BY THE COURT:

22 Q. Agent Alfin, how many times did regalbegal access
23 the Playpen website during the period of time in which
24 the FBI was operating that website?

25 A. I don't know the exact number, your Honor, but I

1 believe he logged onto the website several times, and
2 that period of time was between February 20th, 2015, and
3 March 4th, 2015.

4 I believe -- I believe it was around four or
5 five times, but I would have to look at the report to be
6 sure.

7 Q. All right. Given that there were approximately four
8 or five times when regalbegal accessed Playpen, how many
9 of those occasions was the NIT actually deployed?

10 A. Just once, your Honor. We configured the NIT
11 generally so that after it successfully deployed against
12 a user, we did not deploy it against that user again.

13 Q. What about if a user used a -- created new sign-on
14 credentials for a subsequent visit?

15 A. Then that new account, then it would be possible for
16 them to trigger the NIT again. That did, in fact,
17 happen in a separate investigation, part of the Playpen
18 website.

19 Q. So the NIT was, with respect to regalbegal's access
20 of Playpen, the NIT was deployed one time. Does that
21 mean that only one unique originating number was
22 generated?

23 A. Yes. There was only one unique identifier
24 associated with the regalbegal account.

25 Q. What, to your knowledge -- beyond materiality, is

1 there any reason why the code, the code version of the
2 algorithm that creates the unique identifying numbers,
3 would be sensitive information? Why is that something
4 that would be sensitive?

5 A. With respect to the code that generates the unique
6 identifiers, that code is not particularly sensitive.
7 It's not classified.

8 We generally relied on that part of it being
9 not material. That has been our argument to not provide
10 that information thus far.

11 If the Court finds that that piece of
12 information is material, I will answer that question and
13 disclose it.

14 Q. All right. Do I understand your testimony to be
15 that the NIT code that was provided to the defense was
16 in what you would classify as an assembly language,
17 which is some measure above binary, but that is the only
18 language in which it exists?

19 A. So we gave -- we gave the defendant two separate
20 files. One of them was the binary file, and the
21 separate one was the file containing that assembly
22 language code. And that is -- yes, that is my
23 understanding that is all that exists with respect to
24 source code for the NIT.

25 Q. All right. Is it fair for the Court to assume that

1 the government is not trying to make Mr. Miller's work
2 more difficult for him by failing to disclose a version
3 that would be in a more human-readable format?

4 A. No, there is no -- there is no source code written
5 in any of the friendly formats, C or Java or something
6 of that nature. That particular code, it doesn't exist.
7 We're not withholding it.

8 Q. Are you familiar with the separate counts of the
9 indictment in this case?

10 A. I was present when they were read at the beginning
11 of this hearing, your Honor.

12 Q. Counts One through Four all make reference to on or
13 about March 1st of 2015, that the defendant received
14 visual depictions constituting the exploitation of a
15 minor.

16 Do you know whether or not Counts One through
17 Four pertain to child -- alleged child pornography that
18 the defendant downloaded from the Playpen website while
19 that website was under the government's control?

20 A. I believe that is accurate, your Honor. I would
21 have to -- I would have to verify, but I believe those
22 charges result from downloading child pornography from
23 the Playpen website while it was under government
24 control, yes.

25 Q. The defendant is charged in Count Five with being in

1 possession of contraband images. Do you know whether or
2 not the contraband images charged in Count Five consist
3 of, among other things, the four images identified in
4 Counts One through Four?

5 A. I do not know the answer to that, your Honor, but we
6 can certainly get the answer to it for you.

7 THE COURT: That's all the questions that I
8 have.

9 Does that prompt anything further, Mr. Alfaro?

10 MR. ALFARO: No, your Honor.

11 THE COURT: Mr. Dean?

12 MR. DEAN: No, your Honor.

13 THE COURT: All right. Agent Alfin, you may
14 step down.

15 THE WITNESS: Thank your Honor.

16 THE COURT: Does the government have any
17 further witnesses?

18 MR. DEAN: We do not, your Honor.

19 THE COURT: Any rebuttal, Mr. Alfaro?

20 MR. ALFARO: No rebuttal, your Honor.

21 THE COURT: Well, I'd like to entertain
22 argument at this time as to the materiality issue, and
23 since Mr. Alfaro has the burden on that, I'm going to
24 ask him to go first.

25 MR. ALFARO: Thank your Honor.

1 CLOSING ARGUMENT BY THE DEFENDANT

2 MR. ALFARO: Judge, I believe that we've met
3 our burden in this case. The test for materiality in
4 the Eighth Circuit is whether it's helpful in preparing
5 the defense, or helpful to the defense.

6 It's not -- the burden on us is not are we
7 going to be able to present a defense that's believable;
8 is a jury going to be convinced by our defense; is our
9 defense likely to result in an acquittal.

10 I think the case law, what little is out there
11 for the Eighth Circuit, is certainly that it's much more
12 broader than that. They often come hand in hand when
13 they are talking about Brady, but the Courts are clear
14 to distinguish Brady materiality from Rule 16
15 materiality.

16 So I think that the crux of this case, Judge,
17 is we don't have to take the government's word that the
18 exploit did what it did, that the unique identifiers
19 are, in fact, unique, particularly when we're dealing
20 with this complex technology.

21 I mean, when we look at the most innocent
22 technology in courts around the country like radar gun
23 detectors or BAC alcohol machines, those have to be
24 independently verified and tested and confirmed. So the
25 defendant has a right to a fair trial in this evidence,

1 and it's helpful because it's going to -- it's going to
2 aid the defense in gathering what may be impeachment
3 evidence, rebuttal evidence, and weighed in witness
4 preparation and testimony.

5 I think the Court in Michaud said it best. If
6 it sounds like we're not putting a finer point on it,
7 Judge, I think the Court said it best on why that's so
8 difficult for the defense team.

9 It says that in the government's response to
10 the defense requests in these matters is that the
11 defendant hasn't proved what they do not know. They
12 haven't proved what they do not know, but what they want
13 to know is what they don't know so they can determine
14 what defenses are appropriate.

15 And the Court went on to determine that the
16 defendant has a right to consider the information to
17 determine whether it should lead to a plea agreement or
18 whether there are any favorable defenses, and I think
19 the defendant has a right to that information, and I
20 think that's exactly the position the government is
21 putting us in.

22 They are saying you can't prove that this
23 information will lead to this type of evidence. Well,
24 we can't show that without looking at the code, your
25 Honor. So I think that it's put us in a Catch-22.

1 Additionally the Court in Michaud credited
2 Dr. Miller's testimony in addition to the other
3 declarations that we have submitted to the Court over
4 Agent Alfin's testimony. That's not to say that Agent
5 Alfin isn't being honest.

6 The Court there just makes it clear the
7 defendant is not required to accept the government's
8 assurances that reviewing the NIT code will yield no
9 helpful information, even if the information would yield
10 inculpatory evidence.

11 That evidence may be relevant and helpful to
12 the defense that would render a plan defense useless or
13 alter our own trial strategy or engage in plea
14 discussions, Judge. So by that fact, it is helpful to
15 the defense.

16 In regards to the exploit, the software that
17 generates the unique identifiers and the server
18 component, Agent Alfin has reviewed some of this
19 material, but he didn't write the code, your Honor. He
20 doesn't know all the possibilities that could -- that it
21 could have defects, be flawed or run in a way that it's
22 not intended to, which Dr. Miller said is very common,
23 particularly when we're dealing with complex code.

24 So I think Agent Alfin's testimony should be
25 reviewed skeptically in the sense that he can't verify

1 that because he hasn't analyzed the code itself.

2 I think Dr. Miller sufficiently testified why
3 we need this information. Regarding the unique
4 identifier, we need to review that the algorithm was
5 used to review a unique ID. And just because Agent
6 Alfin says it's unique that we only generated once, on a
7 micro scale that is correct, your Honor. But I believe
8 it's correct to state in the suppression hearing there
9 was a number thrown around that there were at least a
10 thousand users on the website.

11 So we're not talking about just one unique
12 identifier. We're talking about thousands, and I think
13 the increased number creates the risk that this
14 algorithm could operate randomly in unintended
15 consequences that would inappropriately link unique
16 identifiers to a certain individual, and we'll know
17 whether that has, in fact, happened or did not happen by
18 analyzing the code.

19 And I think that same -- that same argument
20 applies to the server component. If that data is stored
21 accurately, then the government has nothing to lose. If
22 it's not -- if it's stored inaccurately, then we can
23 present that argument to the jury that despite this
24 alleged confession, it's helpful for the defense to
25 proffer any reasonable helpful defense that the

1 government's tools were applied inaccurately or have a
2 reasonable probability of malfunctioning.

3 And same is true with the exploit, your Honor.
4 If it is possible for someone to use the exploit to take
5 control over someone's computer or render Mr. Jean's
6 computer in a way that it's vulnerable to attack that
7 could be used as a defense to counterattack whatever the
8 confession may be, that is helpful.

9 We don't need to prove that it's reasonable
10 or -- not reasonable. We don't have to prove that it's
11 going to result in acquittal, but it will be helpful to
12 the defense. We won't know that until we analyze the
13 code, your Honor.

14 So for all these reasons, we believe that this
15 evidence is material. We believe that Mr. Jean has a
16 right to a fair trial in preparing a defense, and we
17 would request that the government enter an order
18 compelling -- that the Court enter an order for the
19 government to compel the code that we've requested.

20 THE COURT: All right. I have a few questions
21 for you. I didn't write down verbatim everything you
22 said about the standard that should be applied to
23 materiality, but just as I was listening to it, I think
24 that I agreed with most, if not everything, that you had
25 to say.

1 Obviously it's the government's burden to prove
2 these charges. The defendant has no burden to prove
3 them. Obviously you don't know what you don't know, and
4 you can't figure out if it's useful until you know; but
5 at some point in gauging what is material from what is
6 merely hypothetical, there has to be some context to
7 gauge that.

8 If this -- if the theory of the defense is that
9 Mr. Jean has been framed, then inside that context, some
10 of the things that you are saying make the discovery of
11 some of this information more material.

12 If that's not a theory of the defense in this
13 case, then it takes what is extremely a remote
14 possibility and making it wholly superfluous because it
15 doesn't matter.

16 What can you tell me -- what are you willing to
17 tell me about the theory of the defense of your case to
18 put the Court in a better position to better understand
19 your materiality argument?

20 MR. ALFARO: And, Judge, I would respond
21 respectfully that that would be an inappropriate
22 consideration for this because the test isn't what type
23 of defense are you going to present and then the Court
24 will determine whether that's relevant or believable.
25 The test is will this evidence be helpful in preparing a

1 defense.

2 THE COURT: That's true.

3 MR. ALFARO: And so I think it would be
4 inappropriate. I don't think I would be able to
5 disclose the theory of defense at this stage. I
6 think -- I think it's fair to say that we could pursue
7 that Mr. Jean was framed. We could also, in addition to
8 doing that, pursuing that, yeah, he confessed, but he
9 was forced to because he didn't know how to explain how
10 his computer was taken over.

11 I mean, in addition to that, I don't even know
12 what other theories of defense I could proffer without
13 reviewing the code. Could I get this evidence and show
14 that there's actually a really reasonably high
15 probability that someone framed him and took over his
16 computer or that the exploit manufactured in a way that
17 it mis- -- that it miscategorized the IP address and
18 linked it to Mr. Jean? I don't know the possibilities
19 and which way --

20 THE COURT: Now, wait a minute. There's been
21 no testimony, that I'm aware of, of a possibility that
22 the exploit has anything to do with the IP address that
23 was returned.

24 MR. ALFARO: Judge, I could be wrong, but I
25 thought part of the testimony was -- let me look at my

1 notes here. I may have been -- one second, your Honor.
2 I think I misspoke.

3 What I was trying to refer to is what we're
4 calling the server component -- the component that
5 generates the unique ID could grab a different username
6 and associate it with a different identification, which
7 would essentially mean this user ID is associated with
8 this IP address that we got back, but it's a
9 miscategory -- mis- -- it's logged incorrectly in being
10 linked to a different defendant, which essentially means
11 that's not his IP address.

12 I don't know if the exploit or the server
13 component that captured it or received it or stored it,
14 were there errors to create that possible error in
15 linkage, if that makes any sense.

16 THE COURT: All right. Well, let's go to some
17 of these specific line items on the exploit. How is it
18 material to your defense? And I agree that this doesn't
19 have to go to your defense. It can merely be, material
20 can be judged by its usefulness in allowing you to
21 cross-examine witnesses or to obtain information that
22 your other witnesses could rely on. But how is it
23 material to know how the government picked the lock on
24 the door, so to speak?

25 MR. ALFARO: Judge, I'm not sure that we agree

1 to that analogy because it's material to know where the
2 government exploited the computer to see if there's
3 flaws there or if it made any changes or altered the
4 security settings such that it's vulnerable to
5 third-party attacks.

6 The government --

7 THE COURT: And why would that -- how would
8 that information --

9 MR. ALFARO: That would --

10 THE COURT: If that happened, how would that
11 affect your defense? What would you argue?

12 MR. ALFARO: I guess potentially that could
13 explain how the child pornography got on the computer.
14 All the government is saying, when it got this, is
15 someone logged in as regalbegal, someone logged in as
16 this person and we think this person was given this
17 unique identifier, and this unique identifier was
18 logged --

19 THE COURT: We're going to get to the unique
20 identifiers in a second. I'm talking about the exploit
21 to the Tor browser.

22 MR. ALFARO: Yeah. Then, your Honor, the
23 exploit -- well, analysis of the exploit code will allow
24 experts to determine, one, that it did -- exactly what
25 it did was pick a lock and not make any changes to the

1 computer.

2 If it did make some sort of change, I can't
3 articulate what that change could be because we don't
4 know. It could have rendered the computer subject to
5 third-party attack that could have resulted in an
6 explanation of why that child pornography is on his
7 computer.

8 THE COURT: Okay. With regard to the -- you've
9 already discussed the unique organizers. Another thing
10 that I understand that you were seeking was, as your
11 witness testified, that it would be very useful to his
12 review to have the, what I've called the NIT code in a
13 source code language rather than binary or assembly
14 language.

15 The government has been -- has testified under
16 oath that it does not exist in a higher level version
17 than the two versions that you've been provided. Are
18 you asking the Court to compel the government to provide
19 something that it's testified it doesn't have, or does
20 that testimony resolve that particular question?

21 MR. ALFARO: It does, your Honor. We weren't
22 specifically requesting that part because we had
23 received that. So that does resolve that issue, your
24 Honor.

25 THE COURT: All right. So we're down to two

1 things, two categorical pieces of information. One is
2 what I have described as the exploit code and the second
3 being the source code that would be associated with how
4 the unique identifying numbers are generated. Those are
5 the two things that you're after at this point that you
6 don't have.

7 MR. ALFARO: That's correct, Judge.

8 THE COURT: Okay. All right. I think I got
9 that part.

10 Mr. Dean?

11 MR. ALFARO: Judge, if I may just have one
12 second --

13 THE COURT: You may.

14 MR. ALFARO: -- to look at the document --

15 THE COURT: Sure.

16 MR. ALFARO: -- in regards to your question
17 regarding the exploit.

18 I would simply direct the Court's attention to
19 Dr. Tsyklevich's declaration as our Defendant's Exhibit
20 A, page 3 of 5, paragraph 6, bullet point number 2, for
21 a more central explanation from the expert that has more
22 experience than myself.

23 THE COURT: One more time.

24 MR. ALFARO: Yes, your Honor. That would be
25 page 3 of 5, Defendant Exhibit A, paragraph 6, bullet

1 point 2. I would just direct the Court's attention to
2 that paragraph for any other clarification. That's all
3 I have, Judge.

4 THE COURT: How do you pronounce that expert's
5 name?

6 MR. ALFARO: I believe it's Tsyklevich.

7 THE COURT: Is he a lawyer?

8 MR. ALFARO: Tsyklevich. Agent Alfin
9 corrected me. I'm sorry. Dr. Tsyklevich. He is not a
10 lawyer, Judge.

11 THE COURT: Why is he opining on a potential
12 admissibility?

13 MR. ALFARO: Oh, it's -- Judge, I guess the
14 Court's question is what could possibility -- what could
15 we possibly discover, or why would it be helpful to get
16 access to the exploit code. And in an abundance of
17 caution, I would just direct the Court to his statement
18 on why, in his expert opinion, the exploit is necessary
19 to be evaluated for the defense.

20 THE COURT: And which bullet point in
21 particular did you say?

22 MR. ALFARO: Bullet point 2.

23 THE COURT: "As noted, --

24 MR. ALFARO: That's correct, your Honor.

25 THE COURT: -- the exploit used"?

1 Why is it that the defense has not engaged a
2 forensic expert to examine Mr. Jean's laptop to come at
3 some of these issues from that direction?

4 MR. ALFARO: Judge, the only response I can say
5 to that is in discussion with the defendant community
6 regarding this case, most individuals who have been
7 consulting with forensic experts seem to agree that
8 because of the significant time span, it's extremely
9 unlikely that any information that could be -- could
10 have been present after the exploit and the NIT were
11 deployed has now been gone because of the process that
12 Dr. Miller referred to, having overwritten data over a
13 period of time.

14 Moreover, experts have informed me that it's
15 entirely possible to write code in such a way that it
16 doesn't leave a trace behind. So the -- given those two
17 explanations, Judge, experts seem more concerned with
18 the fact that, the need to analyze this code to come
19 up -- you know, to evaluate these issues on what the
20 exploit does because it's much more easier to look at a
21 code and say, look at all these paths and say, oh, here
22 it is doing something it's not intended to do versus
23 looking at the computer and seeing what's wrong with the
24 computer.

25 THE COURT: All right. Anything else?

1 MR. ALFARO: No. No, your Honor. Thank you
2 very much.

3 THE COURT: All right. Thank you, Mr. Alfaro.
4 Mr. Dean?

5 MR. DEAN: Thank your Honor.

6 CLOSING ARGUMENT BY THE GOVERNMENT

7 MR. DEAN: First of all, your Honor, I
8 wouldn't -- and I think courts around the country, a
9 couple of courts at least, have not put a whole lot of
10 stock in these declarations from witnesses who were
11 present in the courtroom; subject to cross-examination,
12 I would ask this Court to do the same.

13 I would also ask the Court to not put a whole
14 lot of stock in Dr. Miller's declaration. I think he
15 provided good, sound testimony today, but his
16 declaration is in conflict with some of that testimony.
17 He said in his declaration that was issued: Exploits
18 fundamentally alter a computer. And then when I crossed
19 him on it today, he goes, well, not necessarily; they
20 don't always do that.

21 So you have a very, you know, straightforward
22 statement and then you have a hedging of that.

23 At the end of the day, this defense request is
24 based entirely, 100 percent, on speculation. As Special
25 Agent Alfin testified, there have been over 200 cases

1 prosecuted nationwide that are completely under fire
2 from the defense bar regarding the Playpen website.
3 They are doing their best to find a hole and find an
4 issue in these cases. And to date, not one person has
5 shown that any of these doomsday scenarios or
6 possibilities or what-ifs have occurred anywhere, across
7 the country. Because the whole thing would fall apart,
8 and it hasn't happened.

9 There's no evidence that anything that actually
10 occurred -- that they are saying could have occurred in
11 this case has occurred other than the NIT behaved
12 exactly like it was supposed to do, as it did in this
13 case.

14 Now, the Eighth Circuit is not -- there's not a
15 whole lot of Eighth Circuit case law on the materiality
16 standard, but what's out there says the defense doesn't
17 get to decide it's material. And it's not as Mr. Alfaro
18 said: The standard is a little bit higher than
19 speculation. That's not it. It has to aid the defense,
20 and this in no way aids the defense.

21 THE COURT: But you concede that even if it
22 turns out to be inculpatory evidence that it can still
23 assist the defense in the sense that they don't plow
24 down a path that they shouldn't have taken but don't
25 discover that until it's too late?

1 MR. DEAN: Correct, but they still haven't been
2 able to point to anything other than what-ifs.
3 Dr. Miller's testimony, again, I appreciated his
4 testimony. I thought it was sincere, but it was "could
5 have, might happen, maybe this could happen, you might
6 find this."

7 And then he, himself, said, "You know what?
8 It's even possible that the exploit could have caused
9 unintended consequences on the computer." We heard that
10 several times today.

11 Okay. What did they do with that? They didn't
12 look at a computer. The computer's been sitting in
13 Little Rock this whole time. They don't look at it.
14 They don't want to look at it. Nobody wants to look at
15 the computers across the country.

16 "It's been a long time. Maybe that
17 information's not there anymore." You don't know if you
18 don't try.

19 So for whatever reason they are trying to get
20 this information, I don't think it's for mounting a
21 defense because there's something out there that they
22 could possibly use to mount a defense and they are not
23 doing it. They are ignoring it.

24 And then the chance of an issue, I think when
25 you were inquiring, your Honor, he said, you know, the

1 chance of hacking or something like that. It's above
2 very unlikely, but it's not likely. And then when you
3 confronted him with, well, what about the fact that
4 Mr. Jean in this case actually confessed to being
5 regalbegal, he says, well, then it's much less likely.

6 So then I guess at that point we're much less
7 likely, a little bit above very unlikely. It's fishing.
8 It's speculation. That says it all right there.

9 What's helpful to the defense in this case?
10 What's not helpful to them is the confession by the
11 defendant, and they just kind of push that aside. At
12 the end of the day, you have a NIT that was designed to
13 identify somebody who was downloading child pornography
14 to a certain IP address.

15 We get a subpoena for that IP address from the
16 account regalbegal. We then knock on the door of the
17 person that came back identified as regalbegal, and a
18 man is there that says, "Oh, yeah, how are you doing;
19 I'm regalbegal."

20 The NIT did exactly what it was supposed to do,
21 and everything else is just fishing. It's not going to
22 aid them in any way. They can't come up with any kind
23 of a goofy framing defense or anything else because
24 Mr. Jean said "I'm who you're looking for." NIT set out
25 to look for somebody, we found them, and Mr. Jean

1 confirmed, "Yeah, that's me."

2 I would also, just for the record, like to
3 incorporate all the arguments I made in that suppression
4 hearing for purposes of appeal. Thank your Honor.

5 THE COURT: Do Counts One through Four, the
6 receipt counts in the superseding indictment, are those
7 receipts that the government intends to prove took place
8 by regalbegal from Playpen while it was being monitored
9 by the FBI?

10 MR. DEAN: I believe every single one of those
11 counts is alleged to have occurred on or about March the
12 1st, and based on Special Agent Alfin's testimony, then
13 that would coincide with when it was being monitored by
14 the FBI. It's within that time period.

15 THE COURT: All right.

16 MR. DEAN: So yes.

17 THE COURT: Now, the possession count is
18 alleged more broadly. Does the government anticipate
19 proving that the images that were documented -- or that
20 the government documents in the four receipt counts,
21 that those images were found on the computer several
22 months later when the arrest was made?

23 MR. DEAN: Not necessarily. The possession
24 count that I believe is an "on or about" date in July
25 when the search warrant was executed just reflect the

1 pornography that was found on the computer, on the hard
2 drive, on -- I want to say it's July the 5th, but I'm
3 not sure about that date.

4 THE COURT: It is, and I get that. My question
5 is of the images that were found when the computer
6 was -- when the search warrant was executed, do the four
7 images that are associated with Counts One through Four,
8 were those images part of what they found on the
9 computer?

10 MR. DEAN: Yes, your Honor.

11 THE COURT: All right. Thank you, Mr. Dean.

12 MR. DEAN: Thank your Honor.

13 THE COURT: Anything else you'd like to add,
14 Mr. Alfaro?

15 MR. ALFARO: No, your Honor.

16 THE COURT: All right. The Court is going to
17 take the motion under advisement, and we will get an
18 opinion out as soon as possible. I don't know when that
19 will be, but I would like to think it will be much more
20 quickly than we were able to get out an opinion on the
21 suppression issue because I would like to get this
22 matter pushed forward one way or the other.

23 Based on the evidence before the Court in the
24 theory that Mr. Alfaro has articulated as it relates to
25 this unique identifier and the code that would -- that

1 Dr. Miller has testified that if he had that, he
2 could -- the things he could do with that, I actually
3 have a question for Mr. Alfaro.

4 If the Court ordered the government to produce
5 that code under a protective order, would it be
6 Dr. Miller? Would he be the expert in your stable that
7 would do that work, or do you anticipate someone else?

8 MR. ALFARO: It would be Dr. Miller, your
9 Honor.

10 THE COURT: And do you know of any reason why
11 you would have a need to share that code with anyone
12 else on your defense team or expert team beyond
13 Dr. Miller?

14 MR. ALFARO: Judge, in abundance of caution, I
15 don't want to limit myself. So if the Court were to
16 entertain that order, we would respectfully request that
17 it would be Dr. Miller and an individual with the
18 defense team.

19 I don't anticipate discussing it with anyone
20 else, but I don't want to foreclose the possibility that
21 Dr. Miller would want to consult with another expert.

22 THE COURT: All right. Well, the -- when
23 dealing with protective orders, the less people -- the
24 fewer people that are in the loop I think tends to have
25 somewhat of a correlation between reducing the

1 likelihood that there are any violations, intended or
2 otherwise, or unintended, in the protective order.

3 So to the extent that the Court ultimately
4 orders that, it would likely ask that you limit that,
5 you know, to one expert. And you're telling me that
6 that one on your team of the -- I don't know that
7 they're on your team. You had a different expert at the
8 suppression hearing, and you've attached affidavits from
9 at least a couple of other experts. But you're telling
10 me that Dr. Miller would be the most logical person to
11 get that information?

12 MR. ALFARO: That's correct, your Honor. If
13 the Court did order that, I would seek permission for
14 just Dr. Miller to analyze that, with results.

15 THE COURT: All right. Well, Mr. Dean, would
16 you be willing to do this. Throughout the course of
17 this hearing today, I think we have reduced the
18 discovery dispute from three or four things down to two
19 things: The exploit code and the code that is used to
20 generate the unique identifying number.

21 Given Agent Alfin's testimony about this not
22 being as sensitive as the exploit code, would you confer
23 with your clients and the government and with Mr. Alfaro
24 and try to come to some sort of agreement about that, if
25 possible, with the idea that it would be strictly

1 limited to Dr. Miller's and counsel's eyes only and not
2 to be disseminated beyond that; and after having
3 conferred, let the Court know whether you would be
4 agreeable to that or not?

5 If not, then the Court will rule on both
6 issues, but if you can find some common ground, then
7 that would eliminate the need for the Court to address
8 that issue.

9 MR. DEAN: Your Honor, I'm prepared to do that
10 right now.

11 THE COURT: Very well. Then I would ask the
12 government to refine its protective order so that the
13 code that would be responsible for generating this
14 unique identifying -- unique identifier number could be
15 provided to the defense and that it be at an attorneys'
16 eyes only level, plus Dr. Miller.

17 And Dr. Miller, are you still with us?

18 MR. MILLER: I am.

19 THE COURT: Have you been able to hear what I
20 just ordered?

21 MR. MILLER: Yes, I did.

22 THE COURT: The attorneys will put that order
23 into writing and will effectuate it through a more
24 precise protective order, but I want to make sure you
25 understand that the Court's intent is to give you the

1 information that you have testified could potentially be
2 useful to you in formulating your position on this
3 unique identifier. And you are not to share that
4 information with anyone else, less and except you come
5 back to the Court and get permission. Do you understand
6 that?

7 MR. MILLER: I do understand.

8 THE COURT: All right. Thank you, sir.

9 All right. So if y'all will get together and
10 work on a protective order that contains that language
11 and restrictions, the Court will sign off on it and then
12 we will focus the opinion on whether or not there is,
13 first of all, any materiality that would justify forcing
14 the government to reveal the exploit code. And if the
15 Court answers that question that it is material, then we
16 will set some sort of framework and ask for -- well,
17 we'll sort out the logistics with you of whether we need
18 to have a hearing or whether further confidential
19 briefing, in-camera type briefing or whatever would be
20 sufficient on that. We'll give you more information
21 about that when the order comes out.

22 Anything further today, Mr. Alfaro?

23 MR. ALFARO: No, your Honor. Thank you.

24 THE COURT: Mr. Dean?

25 MR. DEAN: No, your Honor.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

THE COURT: All right. We're adjourned.
(Proceedings adjourned at 5:30 p.m.)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE OF OFFICIAL REPORTER

I, Dana Hayden, Federal Official Realtime Court Reporter, in and for the United States District Court for the Western District of Arkansas, do hereby certify that pursuant to Section 753, Title 28, United States Code that the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Dated this 26th day of October 2016.

Dana Hayden, CCR, RMR, CRR
Federal Official Court Reporter

0	4	115:2, 118:20, 121:19	addition [8] - 15:9, 15:20, 18:21, 21:9, 73:3, 102:2, 106:7, 106:11	120:21
0.27 [3] - 7:18, 53:22, 54:2	4 [1] - 44:24	above-entitled [1] - 124:9	15:20, 18:21, 21:9, 73:3, 102:2, 106:7, 106:11	agents [3] - 4:12, 79:12, 79:15
1	40 [1] - 3:23	absorb [1] - 17:22	106:11	ago [1] - 42:13
1 [1] - 3:3	414 [1] - 1:13	abundance [2] - 111:16, 119:14	106:11	agree [10] - 47:25, 48:1, 51:25, 83:6, 90:3, 93:21, 94:18, 107:18, 107:25, 112:7
100 [3] - 2:17, 50:4, 113:24	42 [1] - 2:9	accept [1] - 102:7	106:11	agreeable [1] - 121:4
100,000 [1] - 88:24	442-2306 [1] - 1:19	access [16] - 13:5, 24:16, 28:22, 32:1, 39:12, 39:15, 40:13, 40:15, 40:17, 40:19, 41:19, 41:24, 54:22, 95:22, 96:19, 111:16	106:11	agreed [1] - 104:24
101 [1] - 43:14	479 [2] - 1:14, 1:19	accessed [3] - 10:11, 89:14, 96:8	106:11	agreement [2] - 101:17, 120:24
11 [3] - 1:9, 2:5, 46:5	4:25 [1] - 90:17	accessing [3] - 3:15, 55:12, 58:19	106:11	ahead [4] - 25:16, 27:18, 37:11, 54:19
113 [1] - 2:18	4:39 [1] - 90:17	accidentally [1] - 61:23	106:11	aid [4] - 78:22, 101:2, 114:19, 116:22
118 [1] - 2:19	4th [1] - 96:3	accompanying [1] - 9:14	106:11	aids [1] - 114:20
123 [1] - 2:20	5	according [3] - 6:22, 7:16, 7:19	106:11	alcohol [1] - 100:23
124 [1] - 2:21	5 [2] - 110:20, 110:25	account [4] - 85:24, 96:15, 96:24, 116:16	106:11	Alfaro [25] - 1:17, 2:9, 2:10, 2:11, 2:14, 3:4, 11:20, 51:5, 53:8, 67:1, 69:13, 69:20, 86:18, 88:18, 90:18, 99:9, 99:19, 99:23, 113:3, 114:17, 118:14, 118:24, 119:3, 120:23, 122:22
13 [1] - 86:13	51 [1] - 2:10	accurate [12] - 41:2, 61:14, 62:13, 71:20, 75:13, 79:6, 88:8, 90:23, 91:1, 91:2, 91:6, 98:20	106:11	ALFARO [61] - 11:24, 12:15, 12:23, 14:15, 15:13, 16:8, 17:2, 18:4, 18:9, 18:12, 19:3, 19:7, 19:15, 20:4, 42:2, 51:6, 51:9, 52:10, 67:3, 67:5, 68:2, 69:9, 69:16, 69:21, 86:19, 86:21, 88:19, 89:8, 89:22, 90:12, 90:20, 95:16, 99:10, 99:20, 99:25, 100:2, 105:20, 106:3, 106:24, 107:25, 108:9, 108:12, 108:22, 109:21, 110:7, 110:11, 110:14, 110:16, 110:24, 111:6, 111:8, 111:13, 111:22, 111:24, 112:4, 113:1, 118:15, 119:8, 119:14, 120:12, 122:23
14 [1] - 86:13	52 [1] - 2:10	accurately [6] - 49:11, 74:18, 75:16, 77:22, 78:15, 103:21	106:11	Alfaro's [1] - 5:2
15 [1] - 90:16	5:15-CR-50087 [1] - 3:3	acknowledges [1] - 73:10	106:11	ALFIN [3] - 2:13, 4:18, 70:3
16 [2] - 11:4, 100:14	5:30 [1] - 123:2	acquired [1] - 48:8	106:11	Alfin [23] - 4:15, 4:19, 5:13, 25:22, 36:1,
1st [2] - 98:13, 117:12	5th [1] - 118:2	acquittal [2] - 100:9, 104:11	106:11	
2	6	actions [1] - 46:10	106:11	
2 [3] - 110:20, 111:1, 111:22	6 [2] - 110:20, 110:25	activating [5] - 6:16, 6:20, 13:3, 52:21, 62:10	106:11	
20 [1] - 2:9	67 [1] - 2:11	active [8] - 55:14, 83:12, 91:17, 91:20, 91:23, 91:25, 93:3, 93:13	106:11	
200 [6] - 88:5, 88:22, 88:23, 88:24, 89:12, 113:25	7	actively [1] - 54:24	106:11	
2003 [2] - 20:25, 21:3	7 [1] - 71:14	activities [1] - 19:1	106:11	
2009 [1] - 70:18	70 [1] - 2:14	activity [5] - 48:13, 76:6, 76:11, 76:22, 84:11	106:11	
2012 [1] - 21:2	72701 [1] - 1:24	actual [15] - 14:3, 14:7, 30:24, 31:7, 43:11, 58:23, 64:12, 64:18, 66:12, 74:10, 74:14, 74:15, 78:12, 80:1, 95:11	106:11	
2013 [1] - 67:10	72703 [1] - 1:19	add [3] - 35:11, 38:20, 118:13	106:11	
2015 [6] - 45:8, 90:22, 91:4, 96:2, 96:3, 98:13	72901 [1] - 1:14		106:11	
2016 [3] - 1:9, 2:5, 124:12	753 [1] - 124:6		106:11	
20th [1] - 96:2	8		106:11	
22nd [1] - 3:11	8,000 [1] - 71:14		106:11	
249-9040 [1] - 1:14	86 [1] - 2:14		106:11	
250 [1] - 88:23	9		106:11	
26th [1] - 124:12	95 [1] - 2:15		106:11	
27 [2] - 73:21, 76:25	9th [1] - 91:3		106:11	
28 [2] - 5:3, 124:6	A		106:11	
280 [1] - 1:18	A-l-f-i-n [1] - 70:11		106:11	
2:14 [1] - 1:9	abilities [1] - 13:18		106:11	
3	ability [2] - 59:17, 87:17		106:11	
3 [3] - 2:6, 110:20, 110:25	able [27] - 10:9, 15:15, 15:17, 15:18, 17:21, 17:22, 26:10, 34:12, 34:13, 41:20, 44:4, 62:9, 64:25, 65:13, 68:21, 68:22, 69:2, 69:3, 83:5, 84:13, 92:9, 100:7, 106:4,		106:11	
30 [1] - 5:4			106:11	
35 [1] - 1:24			106:11	
3739 [1] - 1:18			106:11	

53:17, 69:25, 70:1, 70:10, 71:25, 80:25, 86:22, 88:20, 89:23, 90:21, 91:7, 95:22, 99:13, 102:5, 102:18, 103:6, 111:8, 113:25 Alfin's [5] - 62:4, 102:4, 102:24, 117:12, 120:21 algorithm [7] - 14:21, 16:15, 33:18, 61:18, 97:2, 103:4, 103:14 allegation [1] - 3:17 alleged [10] - 9:12, 50:13, 79:24, 80:19, 80:23, 93:6, 98:17, 103:24, 117:11, 117:18 allegedly [2] - 6:17, 9:22 alleging [1] - 76:20 ALLEN [1] - 1:6 Allen [2] - 3:2, 50:14 allow [7] - 13:7, 21:19, 35:22, 75:17, 93:11, 108:23 allowed [2] - 10:13, 79:6 allowing [1] - 107:20 almost [2] - 31:12, 81:21 alter [3] - 34:21, 102:13, 113:18 alteration [1] - 90:5 altered [3] - 43:22, 45:2, 108:3 altering [1] - 45:25 AMERICA [1] - 1:3 amount [2] - 56:19, 84:23 analogized [1] - 10:14 analogy [2] - 36:21, 108:1 analysis [17] - 20:19, 24:4, 24:9, 25:25, 43:17, 52:18, 61:5, 61:11, 62:7, 68:23, 74:9, 82:1, 82:11, 82:25, 83:6, 86:23, 108:23 analyze [10] - 22:13, 34:1, 34:12, 38:25, 65:13, 68:18, 85:6, 104:12, 112:18, 120:14 analyzed [11] - 27:4, 30:21, 38:7, 52:4, 52:8, 66:9, 72:18, 74:3, 88:22, 93:2,	103:1 analyzing [11] - 37:4, 38:6, 39:2, 39:3, 39:10, 41:8, 41:17, 43:18, 51:11, 91:19, 103:18 anomalies [1] - 86:7 answer [3] - 97:12, 99:5, 99:6 answering [1] - 87:8 answers [1] - 122:15 Anthony [3] - 3:2, 50:14, 72:7 ANTHONY [1] - 1:6 anticipate [6] - 4:16, 5:11, 38:16, 117:18, 119:7, 119:19 anticipates [2] - 4:1, 34:24 anticipating [1] - 38:18 apart [3] - 13:4, 14:5, 114:7 apologize [1] - 89:8 appeal [1] - 117:4 appear [2] - 48:7, 79:22 appeared [1] - 92:23 appearing [2] - 4:5, 20:16 applied [2] - 104:1, 104:22 applies [3] - 11:18, 80:2, 103:20 appreciate [3] - 43:20, 89:6, 89:10 appreciated [1] - 115:3 approach [1] - 70:2 appropriate [2] - 28:4, 101:14 AR [2] - 1:14, 1:19 architected [1] - 40:14 area [2] - 43:16, 44:1 argue [1] - 108:11 ARGUMENT [2] - 100:1, 113:6 Argument [2] - 2:17, 2:18 argument [9] - 80:12, 89:4, 89:6, 89:11, 97:9, 99:22, 103:19, 103:23, 105:19 arguments [1] - 117:3 arising [1] - 25:7 ARKANSAS [2] - 1:1, 1:10 Arkansas [4] - 1:24, 42:18, 42:20, 124:5 arraignment [1] - 9:3	arrest [1] - 117:22 arrested [2] - 88:6, 89:12 articulate [3] - 17:21, 41:24, 109:3 articulated [1] - 118:24 aside [1] - 116:11 aspect [3] - 15:21, 18:13, 69:1 assembly [13] - 22:5, 65:10, 65:24, 68:22, 77:18, 78:3, 78:10, 78:11, 78:14, 97:16, 97:21, 109:13 asserting [1] - 11:12 assertion [1] - 11:17 assets [1] - 56:11 assigned [1] - 70:12 assist [1] - 114:23 assistant [3] - 20:9, 21:9, 42:9 associate [3] - 33:21, 80:15, 107:6 associated [9] - 8:8, 41:4, 43:19, 59:8, 76:20, 96:24, 107:7, 110:3, 118:7 associating [2] - 14:21, 77:1 assume [3] - 4:5, 50:16, 97:25 assuming [1] - 74:19 assumption [1] - 78:6 assurances [1] - 102:8 attached [3] - 5:9, 8:4, 120:8 attachments [1] - 5:5 attack [4] - 35:14, 104:6, 109:5 attacked [1] - 55:5 attacker [1] - 35:17 attacking [1] - 56:14 attacks [1] - 108:5 attention [2] - 110:18, 111:1 attorney [1] - 42:9 Attorney's [1] - 1:13 attorneys [1] - 121:22 attorneys' [1] - 121:15 audience [1] - 58:14 authentication [1] - 48:13 author [2] - 46:6, 72:2 authorized [3] - 72:24, 73:2, 73:13 available [3] - 14:11, 51:23, 59:23 avatar [3] - 6:21, 60:7,	61:15 Avenue [1] - 1:13 aware [9] - 5:15, 47:19, 47:22, 50:12, 50:16, 53:17, 83:22, 87:22, 106:21	B BAC [1] - 100:23 bachelor's [2] - 20:25, 21:3 back-and-forth [1] - 9:5 background [7] - 3:9, 3:18, 3:19, 5:24, 11:20, 58:24, 59:10 bad [3] - 37:8, 37:21, 41:21 banking [1] - 48:13 bar [1] - 114:2 base [1] - 87:10 based [9] - 26:17, 46:10, 48:12, 52:18, 87:20, 92:4, 113:24, 117:12, 118:23 basic [1] - 92:3 basis [2] - 32:22, 78:25 beams [1] - 23:17 bearing [4] - 79:25, 80:13, 80:21, 80:24 became [1] - 77:15 become [1] - 51:15 becoming [1] - 87:12 BEFORE [1] - 1:9 began [2] - 6:23, 9:11 beginning [2] - 29:15, 98:10 begins [1] - 6:11 behalf [3] - 3:4, 3:5, 20:16 behaved [1] - 114:11 behind [3] - 54:8, 94:8, 112:16 believable [2] - 100:7, 105:24 bench [1] - 70:2 benefit [3] - 12:17, 61:21 best [5] - 53:7, 91:2, 101:5, 101:7, 114:3 better [2] - 105:18 between [8] - 9:5, 9:17, 14:3, 71:14, 81:7, 84:1, 96:2, 119:25 beyond [4] - 17:25, 96:25, 119:12, 121:2 big [1] - 38:10	binary [21] - 22:24, 22:25, 23:8, 27:5, 30:24, 31:12, 63:6, 63:17, 64:2, 64:4, 64:7, 64:19, 65:19, 66:1, 68:20, 72:18, 77:17, 78:12, 97:17, 97:20, 109:13 bit [8] - 5:17, 5:24, 23:8, 36:20, 58:16, 65:21, 114:18, 116:7 black [1] - 22:10 blanket [1] - 12:16 blasting [1] - 83:14 blue [4] - 56:11, 56:16, 59:6, 83:5 blueprint [1] - 23:15 Blvd [1] - 1:18 boards [1] - 77:2 boot [1] - 92:11 boot-up [1] - 92:11 booting [1] - 92:14 Brady [2] - 100:13, 100:14 brain [1] - 45:18 break [3] - 12:22, 17:16, 38:19 breezed [1] - 42:15 brief [1] - 90:13 briefing [2] - 122:19 briefly [1] - 20:22 briefs [1] - 5:14 bring [1] - 64:8 broad [1] - 18:1 broader [1] - 100:12 broadly [1] - 117:18 BROOKS [1] - 1:9 brought [1] - 66:9 browser [11] - 7:24, 10:10, 10:15, 13:6, 34:7, 34:24, 53:20, 56:25, 57:4, 82:13, 108:21 browsers [1] - 55:4 building [4] - 23:13, 23:14, 23:15 built [3] - 23:14, 41:6, 92:6 built-in [1] - 92:6 bullet [4] - 110:20, 110:25, 111:20, 111:22 burden [7] - 11:6, 11:18, 99:23, 100:3, 100:6, 105:1, 105:2 Bureau [1] - 70:17 business [2] - 7:17, 56:8 BY [10] - 20:4, 42:7, 51:9, 52:13, 67:5,
---	---	--	---	--	---

70:8, 86:21, 95:21, 100:1, 113:6	112:6, 114:11, 114:13, 114:15, 116:4, 116:9	charges [3] - 3:11, 98:22, 105:2	22:23, 22:24, 22:25, 23:1, 23:5, 23:7, 23:11, 23:20, 24:18, 24:24, 25:4, 25:5, 25:15, 26:2, 26:4, 26:23, 27:2, 27:3, 27:4, 27:7, 28:1, 28:11, 28:14, 28:16, 30:4, 31:2, 31:4, 31:7, 31:11, 31:12, 31:20, 32:8, 32:12, 32:16, 33:4, 33:7, 33:13, 33:18, 34:1, 34:16, 35:4, 35:19, 36:7, 36:8, 36:19, 37:4, 38:6, 38:13, 38:15, 38:20, 39:3, 39:7, 39:10, 40:18, 41:15, 41:17, 41:19, 41:25, 45:23, 52:15, 52:19, 52:20, 57:17, 60:11, 62:19, 63:1, 63:3, 63:4, 63:16, 63:17, 63:19, 64:2, 64:4, 64:7, 64:13, 64:15, 64:18, 64:19, 64:23, 64:25, 65:1, 65:6, 65:19, 65:20, 66:4, 66:6, 66:12, 66:18, 66:20, 66:21, 67:15, 67:21, 68:7, 68:10, 68:13, 68:15, 77:13, 77:17, 77:18, 77:22, 78:1, 78:3, 78:12, 78:16, 78:19, 89:23, 90:1, 90:10, 93:23, 94:10, 94:13, 95:2, 97:1, 97:5, 97:6, 97:15, 97:22, 97:24, 98:4, 98:6, 101:24, 102:8, 102:19, 102:23, 103:1, 103:18, 104:13, 104:19, 106:13, 108:23, 109:12, 109:13, 110:2, 110:3, 111:16, 112:15, 112:18, 112:21, 118:25, 119:5, 119:11, 120:19, 120:22, 121:13, 122:14	coincide [1] - 117:13 colleagues [1] - 81:16 collect [2] - 72:24, 73:14 collected [9] - 7:22, 9:1, 15:1, 18:22, 19:9, 74:4, 74:8, 74:10, 74:18 collection [1] - 21:15 collects [1] - 75:18 coming [2] - 25:1 command [1] - 91:16 commands [1] - 6:16 comments [3] - 64:13, 64:16, 66:2 commerce [1] - 48:13 committing [1] - 85:25 common [5] - 17:11, 33:6, 91:18, 102:22, 121:6 commonly [2] - 77:2, 77:19 commonsense [1] - 89:11 commonsensical [1] - 89:5 communicating [1] - 13:21 communication [3] - 13:23, 73:8, 73:21 communications [1] - 9:5 community [1] - 112:5 company [1] - 21:15 compare [2] - 16:19, 74:16 compared [2] - 49:7, 74:4 comparing [2] - 74:19, 79:8 comparison [2] - 49:13, 86:4 compartments [1] - 23:18 compel [6] - 3:9, 3:25, 5:22, 72:2, 104:19, 109:18 compelling [1] - 104:18 compiler [1] - 63:17 compiling [2] - 31:12, 78:3 complete [3] - 9:8, 12:2, 13:15 completely [4] - 35:20, 77:8, 85:16, 114:1 complex [3] - 33:14, 100:20, 102:23 complicated [1] -
C	Case [1] - 70:14	check [3] - 32:12, 38:13, 57:10		
cache [1] - 28:7 camera [1] - 122:19 capabilities [1] - 85:5 capability [1] - 83:24 capable [1] - 63:14 capacity [1] - 88:21 capture [7] - 31:16, 55:17, 59:15, 85:5, 86:23, 87:23, 95:3 captured [6] - 49:5, 59:16, 83:10, 83:18, 84:17, 107:13 capturing [2] - 59:10, 89:2 car [1] - 36:24 care [1] - 58:13 CASE [1] - 1:5 case [119] - 3:23, 4:13, 5:12, 5:13, 6:13, 6:20, 9:12, 10:6, 18:19, 20:20, 22:3, 22:14, 24:8, 24:10, 24:12, 24:13, 24:17, 24:25, 25:5, 25:8, 25:12, 26:1, 26:4, 26:5, 26:17, 30:17, 33:14, 34:15, 38:21, 40:16, 40:22, 43:1, 43:2, 43:8, 43:12, 44:10, 44:12, 44:22, 45:7, 45:8, 45:13, 45:15, 45:17, 46:1, 46:5, 46:16, 46:19, 50:6, 50:12, 52:3, 52:5, 52:22, 53:18, 60:15, 60:17, 60:19, 61:3, 63:2, 67:12, 67:14, 68:3, 69:18, 70:19, 70:20, 72:8, 74:5, 74:20, 75:9, 75:15, 75:24, 76:15, 78:9, 78:10, 79:7, 80:1, 80:4, 80:9, 80:15, 80:17, 80:22, 81:1, 81:3, 81:9, 81:17, 81:18, 81:22, 81:24, 82:8, 82:9, 82:17, 82:19, 82:24, 82:25, 83:11, 84:6, 84:22, 85:13, 85:16, 85:17, 86:3, 86:12, 87:18, 87:19, 88:7, 90:1, 98:9, 100:3, 100:10, 100:16, 105:13, 105:17,	cases [14] - 4:14, 22:2, 25:7, 59:8, 62:4, 62:7, 66:14, 66:19, 66:23, 71:24, 85:18, 87:21, 113:25, 114:4 Castle [1] - 25:19 Catch-22 [1] - 101:25 catching [1] - 55:8 categorical [1] - 110:1 categorically [1] - 11:22 caught [2] - 67:11, 68:4 caused [3] - 7:3, 9:12, 115:8 caution [2] - 111:17, 119:14 CCR [2] - 1:23, 124:17 central [1] - 110:21 certain [5] - 3:19, 78:2, 92:10, 103:16, 116:14 certainly [6] - 85:23, 86:25, 89:5, 89:6, 99:6, 100:11 CERTIFICATE [1] - 124:1 Certificate [1] - 2:21 certificate [1] - 34:7 certificates [2] - 23:22, 35:12 certify [1] - 124:5 chain [2] - 25:15, 41:9 chance [2] - 115:24, 116:1 change [5] - 45:18, 45:20, 90:4, 109:2, 109:3 changeable [1] - 51:21 changed [6] - 43:22, 45:19, 51:20, 53:13, 57:11, 59:1 changes [13] - 36:4, 45:14, 45:16, 51:18, 52:4, 62:17, 86:23, 92:18, 92:19, 93:1, 93:17, 108:3, 108:25 characteristics [1] - 13:18 characterization [1] - 42:1 characterize [1] - 61:17 charged [2] - 98:25, 99:2	child [16] - 3:16, 6:17, 6:23, 8:21, 9:11, 60:8, 73:16, 84:22, 86:10, 87:12, 98:17, 98:22, 108:13, 109:6, 116:13 children [1] - 21:12 Children [1] - 70:13 Circuit [4] - 100:4, 100:11, 114:14, 114:15 cites [1] - 11:13 city [1] - 36:22 clarification [1] - 111:2 clarify [14] - 11:24, 12:1, 12:3, 12:7, 15:23, 16:21, 18:4, 36:20, 46:14, 68:10, 76:4, 94:12, 94:17, 95:5 classified [1] - 97:7 classify [1] - 97:16 clean [1] - 51:17 clear [6] - 7:13, 13:20, 66:6, 77:15, 100:13, 102:6 clearly [4] - 17:22, 71:8, 75:2, 75:11 clerk [1] - 19:17 CLERK [2] - 19:22, 62:22 client's [1] - 12:17 clients [1] - 120:23 closed [2] - 73:11, 73:20 CLOSING [2] - 100:1, 113:6 Closing [2] - 2:17, 2:18 Code [1] - 124:7 code [195] - 6:14, 6:24, 7:6, 9:9, 10:13, 10:16, 10:23, 10:25, 11:1, 11:3, 11:10, 11:15, 11:23, 12:3, 12:4, 12:6, 12:20, 12:25, 13:2, 13:5, 13:7, 13:9, 13:13, 13:16, 13:22, 13:23, 14:1, 14:16, 15:3, 15:4, 15:11, 15:13, 15:14, 15:21, 15:24, 16:22, 16:25, 17:3, 17:23, 18:6, 22:12, 22:15, 22:16, 22:22,	22:23, 22:24, 22:25, 23:1, 23:5, 23:7, 23:11, 23:20, 24:18, 24:24, 25:4, 25:5, 25:15, 26:2, 26:4, 26:23, 27:2, 27:3, 27:4, 27:7, 28:1, 28:11, 28:14, 28:16, 30:4, 31:2, 31:4, 31:7, 31:11, 31:12, 31:20, 32:8, 32:12, 32:16, 33:4, 33:7, 33:13, 33:18, 34:1, 34:16, 35:4, 35:19, 36:7, 36:8, 36:19, 37:4, 38:6, 38:13, 38:15, 38:20, 39:3, 39:7, 39:10, 40:18, 41:15, 41:17, 41:19, 41:25, 45:23, 52:15, 52:19, 52:20, 57:17, 60:11, 62:19, 63:1, 63:3, 63:4, 63:16, 63:17, 63:19, 64:2, 64:4, 64:7, 64:13, 64:15, 64:18, 64:19, 64:23, 64:25, 65:1, 65:6, 65:19, 65:20, 66:4, 66:6, 66:12, 66:18, 66:20, 66:21, 67:15, 67:21, 68:7, 68:10, 68:13, 68:15, 77:13, 77:17, 77:18, 77:22, 78:1, 78:3, 78:12, 78:16, 78:19, 89:23, 90:1, 90:10, 93:23, 94:10, 94:13, 95:2, 97:1, 97:5, 97:6, 97:15, 97:22, 97:24, 98:4, 98:6, 101:24, 102:8, 102:19, 102:23, 103:1, 103:18, 104:13, 104:19, 106:13, 108:23, 109:12, 109:13, 110:2, 110:3, 111:16, 112:15, 112:18, 112:21, 118:25, 119:5, 119:11, 120:19, 120:22, 121:13, 122:14	22:23, 22:24, 22:25, 23:1, 23:5, 23:7, 23:11, 23:20, 24:18, 24:24, 25:4, 25:5, 25:15, 26:2, 26:4, 26:23, 27:2, 27:3, 27:4, 27:7, 28:1, 28:11, 28:14, 28:16, 30:4, 31:2, 31:4, 31:7, 31:11, 31:12, 31:20, 32:8, 32:12, 32:16, 33:4, 33:7, 33:13, 33:18, 34:1, 34:16, 35:4, 35:19, 36:7, 36:8, 36:19, 37:4, 38:6, 38:13, 38:15, 38:20, 39:3, 39:7, 39:10, 40:18, 41:15, 41:17, 41:19, 41:25, 45:23, 52:15, 52:19, 52:20, 57:17, 60:11, 62:19, 63:1, 63:3, 63:4, 63:16, 63:17, 63:19, 64:2, 64:4, 64:7, 64:13, 64:15, 64:18, 64:19, 64:23, 64:25, 65:1, 65:6, 65:19, 65:20, 66:4, 66:6, 66:12, 66:18, 66:20, 66:21, 67:15, 67:21, 68:7, 68:10, 68:13, 68:15, 77:13, 77:17, 77:18, 77:22, 78:1, 78:3, 78:12, 78:16, 78:19, 89:23, 90:1, 90:10, 93:23, 94:10, 94:13, 95:2, 97:1, 97:5, 97:6, 97:15, 97:22, 97:24, 98:4, 98:6, 101:24, 102:8, 102:19, 102:23, 103:1, 103:18, 104:13, 104:19, 106:13, 108:23, 109:12, 109:13, 110:2, 110:3, 111:16, 112:15, 112:18, 112:21, 118:25, 119:5, 119:11, 120:19, 120:22, 121:13, 122:14

<p>65:21</p> <p>component [29] - 18:21, 29:11, 29:12, 30:6, 32:11, 38:22, 39:1, 39:3, 39:10, 39:21, 40:9, 48:23, 48:24, 49:4, 49:17, 49:22, 49:23, 69:1, 74:13, 74:14, 74:21, 74:23, 90:10, 94:16, 102:18, 103:20, 107:4, 107:13</p> <p>components [7] - 6:3, 6:6, 26:19, 27:11, 31:22, 74:12, 75:5</p> <p>comprised [1] - 71:10</p> <p>compromised [2] - 59:21, 86:7</p> <p>computer [177] - 4:2, 4:4, 6:14, 6:15, 6:20, 6:24, 7:1, 7:2, 7:3, 7:8, 7:15, 7:22, 8:3, 8:10, 9:2, 9:9, 9:11, 9:18, 9:20, 10:1, 10:13, 10:16, 10:17, 12:3, 13:3, 13:15, 13:17, 13:21, 13:22, 13:24, 13:25, 14:4, 16:2, 16:6, 16:7, 16:14, 20:12, 21:4, 21:6, 21:8, 21:17, 21:22, 21:24, 21:25, 22:11, 22:22, 22:25, 23:22, 26:23, 28:15, 28:16, 28:20, 30:4, 30:8, 30:9, 31:2, 31:11, 31:18, 32:18, 32:19, 34:3, 34:11, 34:22, 35:6, 35:10, 35:13, 35:15, 35:19, 35:20, 35:23, 36:3, 36:4, 37:8, 37:9, 37:15, 43:4, 43:7, 43:19, 43:22, 44:15, 44:25, 46:21, 46:25, 48:6, 51:11, 51:15, 51:16, 51:18, 51:23, 52:2, 52:21, 53:2, 53:4, 53:6, 53:15, 53:20, 53:25, 54:2, 54:4, 54:6, 54:9, 54:21, 56:4, 59:21, 60:12, 61:2, 61:5, 61:8, 63:25, 64:1, 66:22, 72:22, 73:6, 73:9, 73:13, 73:16, 73:18, 73:19, 79:4, 79:17, 79:24, 83:25, 84:1, 84:2, 84:7, 84:19, 84:20, 85:7,</p>	<p>90:5, 90:22, 91:3, 91:9, 91:11, 91:13, 91:19, 92:7, 92:17, 92:20, 93:6, 93:7, 93:9, 93:11, 93:12, 93:14, 93:17, 93:20, 94:4, 94:5, 94:7, 94:9, 94:19, 95:15, 104:5, 104:6, 106:10, 106:16, 108:2, 108:13, 109:1, 109:4, 109:7, 112:23, 112:24, 113:18, 115:9, 115:12, 117:21, 118:1, 118:5, 118:9</p> <p>computer's [5] - 7:8, 7:10, 9:13, 13:3, 115:12</p> <p>computers [14] - 6:16, 8:15, 9:22, 14:7, 32:17, 42:25, 43:12, 45:14, 51:20, 62:11, 66:19, 71:11, 71:12, 115:15</p> <p>concede [4] - 81:24, 82:7, 82:17, 114:21</p> <p>concerned [2] - 57:3, 112:17</p> <p>concerns [1] - 26:15</p> <p>conclusion [1] - 50:24</p> <p>conclusions [1] - 78:15</p> <p>condition [1] - 64:24</p> <p>conditions [1] - 66:3</p> <p>conducted [1] - 62:7</p> <p>confer [1] - 120:22</p> <p>Conference [1] - 124:11</p> <p>conferences [1] - 56:18</p> <p>conferred [1] - 121:3</p> <p>conferred [5] - 50:17, 50:20, 80:18, 106:8, 116:4</p> <p>confession [3] - 103:24, 104:8, 116:10</p> <p>confidential [1] - 122:18</p> <p>configuration [3] - 46:9, 92:23, 92:24</p> <p>configurations [2] - 92:20, 92:24</p> <p>configured [3] - 83:25, 92:10, 96:10</p> <p>confirm [2] - 41:1, 74:5</p> <p>confirmed [2] - 100:24, 117:1</p>	<p>conflict [1] - 113:16</p> <p>conformance [1] - 124:10</p> <p>confronted [1] - 116:3</p> <p>confusing [1] - 12:13</p> <p>confusion [1] - 15:22</p> <p>connect [3] - 44:14, 93:11, 93:12</p> <p>connecting [2] - 84:21, 91:24</p> <p>connection [6] - 47:6, 47:14, 48:4, 73:10, 73:11, 73:20</p> <p>connections [6] - 48:11, 91:17, 91:21, 91:25, 93:3, 93:18</p> <p>consequence [1] - 34:5</p> <p>consequences [6] - 33:11, 34:10, 93:22, 94:1, 103:15, 115:9</p> <p>consider [5] - 46:8, 46:16, 55:21, 81:17, 101:16</p> <p>consideration [1] - 105:22</p> <p>considered [1] - 46:17</p> <p>consist [1] - 99:2</p> <p>consisted [1] - 6:14</p> <p>consistent [5] - 44:17, 44:20, 49:13, 50:3, 66:23</p> <p>constitutes [1] - 11:15</p> <p>constituting [1] - 98:14</p> <p>constructed [1] - 23:16</p> <p>consult [2] - 90:14, 119:21</p> <p>consultant [1] - 59:9</p> <p>consulting [2] - 25:12, 112:7</p> <p>contacts [1] - 30:9</p> <p>contained [1] - 72:25</p> <p>containing [1] - 97:21</p> <p>contains [1] - 122:10</p> <p>contends [4] - 8:20, 9:24, 10:1, 11:3</p> <p>content [2] - 58:19, 58:20</p> <p>contention [1] - 60:6</p> <p>contents [1] - 10:1</p> <p>contesting [1] - 18:13</p> <p>context [3] - 60:6, 105:6, 105:9</p> <p>contraband [3] - 10:2, 99:1, 99:2</p> <p>contrasted [1] - 4:24</p> <p>control [10] - 6:19, 35:20, 35:23, 44:15,</p>	<p>47:17, 53:25, 86:13, 98:19, 98:24, 104:5</p> <p>controlling [1] - 54:4</p> <p>converted [1] - 63:25</p> <p>convicted [1] - 100:8</p> <p>Coordination [1] - 70:14</p> <p>copy [5] - 55:1, 64:11, 68:7, 68:9</p> <p>Cornhusker [1] - 24:25</p> <p>corporate [2] - 56:10, 59:7</p> <p>corporations [1] - 59:19</p> <p>correct [56] - 4:9, 4:16, 14:23, 20:17, 20:18, 34:18, 35:15, 37:17, 39:5, 39:19, 41:19, 42:14, 43:1, 43:9, 43:12, 44:22, 44:23, 45:3, 45:9, 48:9, 48:16, 49:5, 50:4, 50:8, 50:11, 50:15, 51:12, 51:13, 52:5, 60:21, 60:24, 61:3, 62:5, 63:5, 63:11, 68:5, 69:4, 71:5, 71:19, 75:7, 77:1, 77:8, 78:19, 83:2, 91:10, 94:4, 94:23, 95:8, 103:7, 103:8, 110:7, 111:24, 115:1, 120:12, 124:7</p> <p>corrected [2] - 51:19, 111:9</p> <p>correction [1] - 47:16</p> <p>correctly [2] - 60:24, 62:6</p> <p>correlate [1] - 76:22</p> <p>correlated [2] - 32:5, 76:7</p> <p>correlating [1] - 76:12</p> <p>correlation [1] - 119:25</p> <p>Cottom [22] - 22:3, 22:14, 24:8, 34:15, 40:16, 45:7, 45:8, 46:5, 47:4, 47:13, 52:3, 60:15, 60:19, 69:3, 81:1, 81:9, 81:11, 82:4, 82:8, 82:9, 82:20, 82:25</p> <p>counsel [2] - 5:7, 9:5</p> <p>counsel's [1] - 121:1</p> <p>Count [2] - 98:25, 99:2</p> <p>count [4] - 3:13, 3:15, 117:17, 117:24</p> <p>counterattack [1] -</p>	<p>104:7</p> <p>countermeasures [1] - 55:23</p> <p>country [6] - 4:15, 71:23, 100:22, 113:8, 114:7, 115:15</p> <p>counts [6] - 3:11, 98:8, 98:12, 117:6, 117:11, 117:20</p> <p>Counts [4] - 98:16, 99:4, 117:5, 118:7</p> <p>couple [3] - 42:12, 113:9, 120:9</p> <p>course [1] - 120:16</p> <p>courses [1] - 24:2</p> <p>Court [67] - 1:23, 2:6, 2:10, 2:15, 2:20, 2:21, 3:18, 3:24, 4:23, 6:1, 6:2, 6:14, 8:16, 8:17, 8:24, 9:6, 10:3, 11:10, 11:25, 12:1, 18:14, 20:23, 21:10, 26:10, 30:20, 57:14, 57:17, 67:6, 67:24, 69:17, 70:9, 70:22, 71:2, 72:6, 73:21, 75:11, 75:15, 97:11, 97:25, 101:5, 101:7, 101:15, 102:1, 102:3, 102:6, 104:18, 105:18, 105:23, 109:18, 111:17, 113:12, 113:13, 118:16, 118:23, 119:4, 119:15, 120:3, 120:13, 121:3, 121:5, 121:7, 122:5, 122:11, 122:15, 124:3, 124:4, 124:17</p> <p>count [2] - 5:3, 5:5</p> <p>COURT [86] - 1:1, 3:1, 3:8, 4:10, 4:19, 12:12, 12:16, 12:24, 15:8, 15:20, 16:24, 17:8, 18:8, 18:11, 18:25, 19:5, 19:12, 19:17, 19:20, 42:3, 42:5, 51:4, 51:7, 52:11, 52:13, 62:24, 67:1, 67:24, 69:10, 69:13, 69:19, 69:22, 70:1, 70:5, 86:17, 88:18, 89:4, 89:10, 90:15, 90:18, 95:17, 95:21, 99:7, 99:11, 99:13, 99:16, 99:19, 99:21, 104:20, 106:2, 106:20, 107:16, 108:7,</p>
---	---	--	---	--

<p>108:10, 108:19, 109:8, 109:25, 110:8, 110:13, 110:15, 110:23, 111:4, 111:7, 111:11, 111:20, 111:23, 111:25, 112:25, 113:3, 114:21, 117:5, 117:15, 117:17, 118:4, 118:11, 118:13, 118:16, 119:10, 119:22, 120:15, 121:11, 121:19, 121:22, 122:8, 122:24, 123:1</p> <p>Court's [9] - 3:22, 4:22, 7:5, 10:7, 75:13, 110:18, 111:1, 111:14, 121:25</p> <p>courtroom [1] - 113:11</p> <p>Courts [1] - 100:13</p> <p>courts [4] - 71:22, 100:22, 113:8, 113:9</p> <p>CRAIG [2] - 19:22, 62:22</p> <p>crash [1] - 35:5</p> <p>create [13] - 14:17, 14:18, 16:15, 22:24, 23:7, 27:12, 27:13, 31:5, 31:7, 77:13, 94:22, 107:14</p> <p>created [7] - 14:20, 15:1, 21:18, 21:19, 28:19, 33:22, 96:13</p> <p>creates [4] - 15:5, 33:19, 97:2, 103:13</p> <p>creating [2] - 27:21, 31:5</p> <p>credentials [1] - 96:14</p> <p>credibility [1] - 88:24</p> <p>credible [1] - 62:13</p> <p>credited [1] - 102:1</p> <p>crime [1] - 85:25</p> <p>Crimes [1] - 70:13</p> <p>criminal [1] - 66:15</p> <p>Criminal [1] - 70:12</p> <p>critical [1] - 48:12</p> <p>criticism [2] - 64:3, 64:17</p> <p>CROSS [2] - 42:6, 86:20</p> <p>cross [4] - 43:14, 51:10, 107:21, 113:11</p> <p>Cross [2] - 2:9, 2:14</p> <p>cross-examination [2] - 51:10, 113:11</p>	<p>CROSS-EXAMINATION [2] - 42:6, 86:20</p> <p>Cross-Examination [2] - 2:9, 2:14</p> <p>cross-examine [1] - 107:21</p> <p>crossed [1] - 113:18</p> <p>CRR [2] - 1:23, 124:17</p> <p>crux [1] - 100:16</p> <p>current [2] - 3:24, 72:1</p> <p>customers [1] - 21:19</p> <p>cut [1] - 25:24</p> <p>cyber [1] - 20:12</p>	<p>118:11, 120:15, 122:24</p> <p>DEAN [25] - 4:17, 42:4, 42:7, 51:3, 62:21, 67:20, 69:11, 69:24, 70:6, 70:8, 86:16, 88:14, 95:19, 99:12, 99:18, 113:5, 113:7, 115:1, 117:10, 117:16, 117:23, 118:10, 118:12, 121:9, 122:25</p> <p>debug [1] - 23:3</p> <p>decide [2] - 41:20, 114:17</p> <p>decided [1] - 21:13</p> <p>declaration [12] - 25:17, 25:18, 25:21, 44:21, 44:24, 72:2, 90:8, 91:7, 110:19, 113:14, 113:16, 113:17</p> <p>declarations [2] - 102:3, 113:10</p> <p>deeply [1] - 8:17</p> <p>default [2] - 92:20, 92:24</p> <p>defaults [1] - 92:6</p> <p>defect [2] - 41:10, 41:11</p> <p>defects [6] - 33:4, 38:4, 41:7, 41:9, 41:24, 102:21</p> <p>defend [2] - 56:13, 59:14</p> <p>defendant [25] - 1:7, 3:3, 4:1, 11:6, 15:6, 15:7, 50:14, 72:7, 72:9, 75:6, 75:8, 92:5, 97:19, 98:13, 98:18, 98:25, 100:25, 101:11, 101:16, 101:19, 102:7, 105:2, 107:10, 112:5, 116:11</p> <p>Defendant [2] - 2:17, 110:25</p> <p>DEFENDANT [3] - 1:16, 3:7, 100:1</p> <p>defendant's [7] - 3:22, 3:25, 51:11, 60:18, 70:24, 79:17, 110:19</p> <p>DEFENDANT'S [1] - 2:7</p> <p>Defender [1] - 1:18</p> <p>defense [78] - 5:21, 6:5, 7:21, 9:4, 11:5, 11:11, 12:18, 12:19,</p>	<p>20:16, 25:18, 26:11, 29:9, 29:16, 31:25, 34:1, 38:25, 49:9, 60:18, 60:23, 61:1, 68:6, 68:9, 68:18, 68:25, 73:24, 75:12, 75:14, 75:20, 75:23, 77:10, 78:20, 78:22, 79:18, 81:21, 85:15, 97:15, 100:5, 100:7, 100:8, 100:9, 101:2, 101:8, 101:10, 102:12, 102:15, 103:24, 103:25, 104:7, 104:12, 104:16, 105:8, 105:12, 105:17, 105:23, 106:1, 106:5, 106:12, 107:18, 107:19, 108:11, 111:19, 112:1, 113:23, 114:2, 114:16, 114:19, 114:20, 114:23, 115:21, 115:22, 116:9, 116:23, 119:12, 119:18, 121:15</p> <p>defenses [2] - 101:14, 101:18</p> <p>defined [3] - 6:8, 17:17, 17:18</p> <p>definite [2] - 35:7, 57:2</p> <p>definitely [3] - 35:17, 57:11, 59:3</p> <p>definition [1] - 45:22</p> <p>degrade [1] - 52:1</p> <p>degree [1] - 89:18</p> <p>delete [2] - 61:8, 61:10</p> <p>deleted [1] - 51:19</p> <p>Denis [3] - 1:12, 3:3, 42:8</p> <p>Denis.Dean@usdoj.gov [1] - 1:15</p> <p>depictions [1] - 98:14</p> <p>deploy [1] - 96:12</p> <p>deployed [11] - 31:24, 67:16, 86:2, 86:12, 88:10, 88:12, 89:13, 96:9, 96:11, 96:20, 112:11</p> <p>describe [9] - 5:19, 18:1, 20:22, 22:9, 26:18, 44:8, 44:9, 64:14, 72:6</p> <p>described [18] - 6:18, 7:13, 8:1, 9:15, 10:14, 10:21, 14:13, 16:25, 26:20, 52:16,</p>	<p>52:19, 57:21, 59:6, 63:4, 75:16, 75:23, 94:16, 110:2</p> <p>describes [1] - 26:8</p> <p>describing [2] - 6:5, 81:13</p> <p>description [2] - 79:5, 85:14</p> <p>descriptive [2] - 63:20, 63:21</p> <p>design [1] - 37:25</p> <p>designed [3] - 14:1, 46:22, 116:12</p> <p>desired [1] - 59:18</p> <p>despite [1] - 103:23</p> <p>destination [1] - 84:8</p> <p>destroyed [1] - 40:20</p> <p>detail [1] - 9:22</p> <p>detectors [1] - 100:23</p> <p>determine [8] - 13:24, 34:13, 57:17, 101:13, 101:15, 101:17, 105:24, 108:24</p> <p>determined [1] - 49:9</p> <p>develop [1] - 59:4</p> <p>device [1] - 32:18</p> <p>difference [4] - 81:7, 82:3, 82:5, 85:18</p> <p>different [37] - 6:3, 6:4, 16:21, 23:17, 28:21, 33:21, 36:12, 36:13, 36:23, 36:25, 37:2, 37:12, 37:18, 37:20, 38:4, 38:14, 38:16, 41:14, 48:24, 56:17, 59:7, 63:22, 63:23, 64:25, 65:11, 65:17, 66:3, 66:4, 67:16, 67:21, 76:12, 86:3, 107:5, 107:6, 107:10, 120:7</p> <p>difficult [10] - 23:10, 23:18, 41:23, 64:7, 64:9, 64:20, 80:6, 80:8, 98:2, 101:8</p> <p>digital [1] - 43:1</p> <p>DIRECT [2] - 20:3, 70:7</p> <p>Direct [2] - 2:9, 2:14</p> <p>direct [4] - 44:8, 110:18, 111:1, 111:17</p> <p>direction [1] - 112:3</p> <p>directly [1] - 8:13</p> <p>directories [1] - 92:12</p> <p>directory [3] - 92:7, 92:11</p> <p>disable [3] - 35:10, 35:11, 90:5</p>
D				
	<p>Dakota [2] - 22:4, 24:7</p> <p>Dana [3] - 1:23, 124:3, 124:17</p> <p>Daniel [2] - 69:24, 70:10</p> <p>DANIEL [2] - 2:13, 70:3</p> <p>data [66] - 9:17, 12:4, 13:11, 13:20, 14:3, 18:23, 18:25, 19:3, 19:5, 19:10, 25:1, 29:4, 29:6, 31:15, 39:5, 39:23, 39:25, 41:5, 44:16, 44:17, 47:5, 47:15, 47:20, 48:8, 48:11, 48:23, 49:4, 49:8, 49:10, 51:14, 51:17, 55:17, 66:23, 66:24, 73:1, 73:4, 73:7, 73:10, 74:7, 74:8, 74:10, 74:14, 74:15, 74:18, 74:21, 74:22, 74:23, 74:24, 75:1, 75:18, 76:15, 84:4, 84:7, 84:12, 84:23, 85:6, 95:11, 95:13, 103:20, 112:12</p> <p>database [1] - 39:24</p> <p>datasets [3] - 49:16, 49:21, 74:19</p> <p>date [5] - 90:24, 91:5, 114:4, 117:24, 118:3</p> <p>Dated [1] - 124:12</p> <p>days [1] - 86:13</p> <p>dealing [4] - 43:8, 100:19, 102:23, 119:23</p> <p>deals [1] - 44:7</p> <p>Dean [13] - 1:12, 2:9, 2:14, 3:3, 42:8, 69:10, 69:22, 99:11, 110:10, 113:4,</p>			

<p>disabled [2] - 34:6, 43:23</p> <p>disassembly [1] - 31:3</p> <p>disclose [3] - 97:13, 98:2, 106:5</p> <p>disclosed [1] - 9:21</p> <p>disclosure [1] - 11:14</p> <p>disconnect [1] - 5:18</p> <p>discover [2] - 111:15, 114:25</p> <p>discoverable [1] - 11:4</p> <p>discovery [8] - 3:25, 4:23, 9:4, 11:8, 49:9, 79:23, 105:10, 120:18</p> <p>discussed [2] - 69:1, 109:9</p> <p>discussing [1] - 119:19</p> <p>discussion [2] - 83:5, 112:5</p> <p>discussions [1] - 102:14</p> <p>displayed [1] - 95:3</p> <p>dispute [8] - 4:23, 6:10, 10:6, 10:8, 15:10, 19:14, 50:25, 120:18</p> <p>disseminated [1] - 121:2</p> <p>distinguish [1] - 100:14</p> <p>District [2] - 124:4, 124:5</p> <p>DISTRICT [2] - 1:1, 1:1</p> <p>Division [1] - 70:13</p> <p>docket [2] - 3:2, 60:17</p> <p>Doctor [2] - 51:2, 51:10</p> <p>doctor [1] - 43:10</p> <p>doctorate [1] - 21:2</p> <p>Document [2] - 5:3, 5:4</p> <p>document [2] - 3:23, 110:14</p> <p>documented [2] - 18:25, 117:19</p> <p>documents [3] - 26:5, 26:18, 117:20</p> <p>done [11] - 25:11, 38:7, 38:8, 54:4, 56:3, 57:2, 57:8, 72:19, 79:17, 80:9</p> <p>doomsday [1] - 114:5</p> <p>door [7] - 10:15, 13:6, 53:19, 54:14, 67:24, 107:24, 116:16</p> <p>doorstep [1] - 8:14</p> <p>doorways [1] - 23:17</p>	<p>doubt [1] - 53:5</p> <p>down [10] - 12:22, 24:21, 37:1, 37:2, 89:19, 99:14, 104:21, 109:25, 114:24, 120:18</p> <p>download [2] - 6:23, 60:20</p> <p>downloaded [5] - 6:17, 9:23, 14:8, 60:8, 98:18</p> <p>downloading [7] - 8:20, 9:11, 54:1, 61:16, 84:22, 98:22, 116:13</p> <p>Dr [50] - 12:7, 16:20, 16:23, 17:7, 18:23, 19:8, 19:10, 19:16, 20:5, 20:7, 20:8, 25:19, 42:8, 47:19, 67:6, 72:18, 72:19, 74:9, 76:2, 77:1, 77:16, 77:21, 77:23, 79:5, 79:20, 79:21, 80:25, 81:15, 81:19, 83:1, 90:14, 102:2, 102:22, 103:2, 110:19, 111:9, 112:12, 113:14, 115:3, 119:1, 119:6, 119:8, 119:13, 119:17, 119:21, 120:10, 120:14, 121:1, 121:16, 121:17</p> <p>DR [1] - 2:8</p> <p>drawn [1] - 86:5</p> <p>drive [2] - 36:22, 118:2</p> <p>drove [1] - 42:20</p> <p>duly [3] - 19:24, 20:2, 70:4</p> <p>duplicated [1] - 39:6</p> <p>during [7] - 4:11, 12:7, 27:10, 36:17, 76:24, 90:24, 95:23</p>	<p>effort [2] - 60:20, 66:11</p> <p>Eighth [4] - 100:4, 100:11, 114:14, 114:15</p> <p>either [8] - 8:18, 28:7, 57:2, 66:18, 66:19, 78:11, 92:23, 94:6</p> <p>eliminate [1] - 121:7</p> <p>employ [1] - 55:23</p> <p>employed [3] - 20:8, 20:13, 70:16</p> <p>enabled [1] - 79:4</p> <p>enables [1] - 81:5</p> <p>encrypted [5] - 47:21, 84:5, 84:7, 84:8, 84:12</p> <p>encryption [2] - 47:4, 84:7</p> <p>end [11] - 46:11, 57:25, 62:2, 74:24, 74:25, 78:3, 84:6, 85:1, 113:23, 116:12</p> <p>end-to-end [1] - 84:6</p> <p>ends [4] - 34:25, 37:2, 73:8, 75:2</p> <p>enforcement [2] - 11:13, 82:23</p> <p>enforcement-sensitive [1] - 82:23</p> <p>engage [1] - 102:13</p> <p>engaged [1] - 112:1</p> <p>engineer [7] - 22:11, 22:15, 22:17, 22:21, 23:10, 23:19, 68:21</p> <p>Engineer [1] - 35:22</p> <p>engineered [2] - 14:1, 27:5</p> <p>engineering [8] - 22:3, 22:5, 23:4, 24:2, 24:5, 37:6, 37:22, 38:5</p> <p>English [1] - 47:2</p> <p>enter [3] - 79:10, 104:17, 104:18</p> <p>entered [1] - 79:12</p> <p>entertain [2] - 99:21, 119:16</p> <p>entire [8] - 12:20, 21:19, 21:20, 25:15, 27:10, 41:3, 41:6, 41:9</p> <p>entirely [2] - 112:15, 113:24</p> <p>entirety [4] - 13:3, 13:9, 30:13, 30:14</p> <p>entitled [1] - 124:9</p> <p>entry [1] - 79:8</p> <p>environment [2] - 52:16, 66:22</p>	<p>environments [1] - 59:7</p> <p>error [7] - 32:15, 33:6, 33:20, 35:7, 47:16, 93:22, 107:14</p> <p>errors [12] - 32:12, 33:4, 33:7, 33:14, 33:17, 34:19, 37:25, 39:7, 39:8, 41:21, 62:19, 107:14</p> <p>especially [1] - 59:14</p> <p>essentially [2] - 107:7, 107:10</p> <p>establish [2] - 11:6, 11:18</p> <p>ethical [1] - 55:22</p> <p>evaluate [1] - 112:19</p> <p>evaluated [1] - 111:19</p> <p>event [1] - 11:12</p> <p>eventually [1] - 51:18</p> <p>evidence [26] - 4:21, 10:2, 10:5, 43:1, 43:2, 43:4, 60:13, 60:19, 61:21, 72:7, 72:13, 79:13, 80:1, 85:12, 100:25, 101:3, 101:23, 102:10, 102:11, 104:15, 105:25, 106:13, 114:9, 114:22, 118:23</p> <p>evidentiary [1] - 8:25</p> <p>evolved [1] - 66:14</p> <p>exact [4] - 49:14, 90:24, 91:5, 95:25</p> <p>exactly [7] - 27:6, 40:13, 50:1, 101:20, 108:24, 114:12, 116:20</p> <p>exaggerating [1] - 58:15</p> <p>Examination [8] - 2:9, 2:10, 2:10, 2:11, 2:14, 2:14, 2:15</p> <p>examination [2] - 51:10, 113:11</p> <p>EXAMINATION [8] - 20:3, 42:6, 51:8, 52:12, 67:4, 70:7, 86:20, 95:20</p> <p>examine [4] - 44:9, 57:15, 107:21, 112:2</p> <p>examined [3] - 52:15, 53:1</p> <p>example [2] - 23:12, 64:10</p> <p>examples [1] - 33:9</p> <p>exceed [2] - 72:15, 74:1</p> <p>except [1] - 122:4</p>	<p>exchange [1] - 26:10</p> <p>exchanged [4] - 5:7, 13:11, 13:20, 73:11</p> <p>excused [1] - 69:14</p> <p>execute [2] - 16:13, 79:9</p> <p>executed [8] - 8:15, 9:19, 36:25, 45:14, 45:21, 72:18, 117:25, 118:6</p> <p>execution [8] - 8:18, 36:9, 36:10, 36:13, 38:3, 73:5, 75:17, 95:14</p> <p>exemption [1] - 87:12</p> <p>Exhibit [2] - 110:19, 110:25</p> <p>exist [6] - 35:9, 39:8, 39:14, 78:18, 98:6, 109:16</p> <p>exists [5] - 5:20, 12:21, 68:16, 97:18, 97:23</p> <p>expect [1] - 92:15</p> <p>expected [1] - 34:24</p> <p>experience [10] - 22:6, 23:21, 26:16, 31:25, 33:24, 38:6, 38:24, 40:24, 87:20, 110:22</p> <p>experiment [2] - 52:16, 52:17</p> <p>expert [21] - 4:2, 5:15, 7:19, 7:20, 7:21, 13:8, 17:20, 24:9, 25:17, 28:15, 43:25, 47:13, 81:1, 110:21, 111:18, 112:2, 119:6, 119:12, 119:21, 120:5, 120:7</p> <p>expert's [1] - 111:4</p> <p>expertise [7] - 43:16, 44:1, 44:7, 87:4, 87:17, 87:23, 88:4</p> <p>experts [13] - 6:5, 13:17, 14:18, 16:10, 18:6, 27:8, 43:11, 81:21, 108:24, 112:7, 112:14, 112:17, 120:9</p> <p>explain [15] - 16:9, 16:23, 18:23, 22:20, 25:10, 29:23, 30:20, 31:25, 33:24, 34:21, 38:25, 40:25, 78:25, 106:9, 108:13</p> <p>explained [3] - 52:14, 62:15, 89:20</p> <p>explaining [1] - 5:23</p> <p>explanation [2] - 109:6, 110:21</p>
	E			
<p>e-mails [1] - 5:7</p> <p>early [1] - 77:16</p> <p>easier [2] - 23:13, 112:20</p> <p>East [1] - 1:24</p> <p>easy [4] - 65:14, 77:25, 78:1, 78:4</p> <p>educate [1] - 18:14</p> <p>education [1] - 20:22</p> <p>effect [2] - 7:25, 40:21</p> <p>effects [1] - 91:23</p> <p>effectuate [1] - 121:23</p>				

<p>explanations [1] - 112:17</p> <p>exploit [120] - 10:10, 10:19, 10:21, 10:22, 11:1, 11:2, 11:10, 11:14, 11:22, 16:24, 16:25, 17:19, 18:19, 25:14, 26:22, 28:19, 28:24, 30:7, 34:1, 34:2, 34:4, 34:12, 34:21, 34:23, 35:2, 35:5, 35:25, 36:3, 36:17, 37:10, 37:15, 37:24, 44:2, 45:23, 46:17, 46:24, 52:6, 52:24, 54:11, 54:12, 54:13, 54:22, 54:24, 55:1, 55:4, 55:9, 55:17, 57:7, 57:16, 67:11, 68:4, 68:10, 68:12, 68:13, 68:19, 68:20, 75:15, 75:16, 75:19, 78:22, 79:2, 79:3, 79:6, 79:25, 81:3, 81:4, 81:6, 81:8, 81:12, 81:14, 81:18, 81:19, 82:3, 82:5, 82:10, 83:11, 83:13, 83:18, 83:23, 84:14, 84:18, 84:24, 85:4, 85:7, 86:1, 86:2, 86:12, 86:24, 87:24, 88:22, 90:1, 90:4, 91:8, 91:9, 93:23, 100:18, 102:16, 104:3, 104:4, 106:16, 106:22, 107:12, 107:17, 108:20, 108:23, 110:2, 110:17, 111:16, 111:18, 111:25, 112:10, 112:20, 115:8, 120:19, 120:22, 122:14</p> <p>exploit-type [1] - 81:8</p> <p>exploitation [4] - 3:12, 3:14, 46:11, 98:14</p> <p>exploited [3] - 45:1, 46:9, 108:2</p> <p>exploiting [1] - 46:20</p> <p>exploits [7] - 35:9, 68:14, 82:3, 86:8, 90:8, 93:24, 113:17</p> <p>extent [5] - 11:16, 61:13, 62:1, 62:13, 120:3</p> <p>extremely [3] - 89:3, 105:13, 112:8</p> <p>eyes [2] - 121:1,</p>	<p>121:16</p> <p style="text-align: center;">F</p> <p>Facebook [2] - 58:12, 58:13</p> <p>facing [1] - 3:10</p> <p>fact [20] - 32:19, 45:24, 47:5, 47:21, 50:20, 52:15, 59:12, 59:16, 69:6, 70:22, 71:7, 80:4, 80:22, 86:22, 96:16, 100:19, 102:14, 103:17, 112:18, 116:3</p> <p>facts [1] - 11:18</p> <p>factually [1] - 71:20</p> <p>failed [3] - 49:17, 49:22, 74:21</p> <p>failing [1] - 98:2</p> <p>failure [1] - 80:12</p> <p>fair [11] - 48:22, 49:12, 50:5, 51:2, 56:19, 68:1, 82:20, 97:25, 100:25, 104:16, 106:6</p> <p>fairly [6] - 33:6, 48:2, 55:19, 55:21, 65:14, 66:10</p> <p>faith [1] - 66:11</p> <p>fall [2] - 57:25, 114:7</p> <p>familiar [14] - 25:7, 25:10, 51:14, 65:4, 65:7, 65:8, 65:16, 67:10, 67:14, 67:22, 80:25, 87:21, 88:3, 98:8</p> <p>far [5] - 23:24, 41:1, 72:10, 78:17, 97:10</p> <p>farfetched [1] - 85:11</p> <p>fashion [1] - 7:14</p> <p>favorable [1] - 101:18</p> <p>FAYETTEVILLE [1] - 1:10</p> <p>Fayetteville [2] - 1:19, 1:24</p> <p>FBI [18] - 4:12, 10:9, 10:12, 42:22, 46:17, 50:6, 50:13, 50:22, 54:23, 58:5, 63:13, 70:11, 70:12, 70:18, 86:13, 95:24, 117:9, 117:14</p> <p>FBI's [6] - 6:12, 6:13, 83:11, 83:18, 83:22, 85:3</p> <p>feature [1] - 93:19</p> <p>February [1] - 96:2</p> <p>Federal [5] - 1:18,</p>	<p>1:23, 70:16, 124:3, 124:17</p> <p>few [4] - 33:2, 51:6, 90:20, 104:20</p> <p>fewer [1] - 119:24</p> <p>field [3] - 4:2, 18:7, 55:22</p> <p>figure [3] - 23:16, 59:20, 105:4</p> <p>file [20] - 3:23, 5:3, 5:5, 24:15, 24:22, 27:5, 29:6, 30:24, 31:3, 40:1, 40:4, 43:19, 44:18, 72:18, 92:11, 93:20, 95:4, 95:6, 97:20, 97:21</p> <p>filed [2] - 3:10, 5:6</p> <p>filenames [1] - 92:9</p> <p>files [8] - 49:3, 51:17, 61:6, 92:7, 92:21, 92:23, 93:2, 97:20</p> <p>findings [1] - 3:21</p> <p>fine [1] - 69:19</p> <p>finer [1] - 101:6</p> <p>finish [1] - 87:8</p> <p>fire [1] - 114:1</p> <p>firewall [5] - 34:6, 35:11, 35:16, 90:6, 92:17</p> <p>first [21] - 12:1, 12:10, 14:1, 15:10, 20:2, 28:24, 29:19, 29:20, 32:1, 70:4, 79:2, 81:11, 83:11, 83:17, 83:21, 84:9, 91:13, 91:16, 99:24, 113:7, 122:13</p> <p>firsthand [1] - 84:25</p> <p>fishing [2] - 116:7, 116:21</p> <p>Five [2] - 98:25, 99:2</p> <p>five [4] - 21:14, 66:10, 96:5, 96:8</p> <p>fix [1] - 38:20</p> <p>flash [4] - 24:14, 24:15, 46:20, 46:23</p> <p>flaw [2] - 34:3, 46:20</p> <p>flawed [1] - 102:21</p> <p>flaws [3] - 35:3, 37:25, 108:3</p> <p>flow [2] - 23:2, 47:16</p> <p>focus [1] - 122:12</p> <p>follow [1] - 49:7</p> <p>following [2] - 9:3, 9:7</p> <p>follows [2] - 20:2, 70:4</p> <p>followup [1] - 68:1</p> <p>FOR [2] - 1:11, 1:16</p> <p>forced [1] - 106:9</p> <p>forcing [1] - 122:13</p> <p>foreclose [1] - 119:20</p>	<p>foregoing [1] - 124:7</p> <p>forensic [6] - 4:3, 43:17, 43:24, 45:7, 112:2, 112:7</p> <p>forfeiture [1] - 3:16</p> <p>form [1] - 63:20</p> <p>format [7] - 12:8, 63:6, 64:5, 69:5, 85:8, 98:3, 124:10</p> <p>formats [1] - 98:5</p> <p>formulating [1] - 122:2</p> <p>Fort [1] - 1:14</p> <p>forth [4] - 5:8, 9:5, 13:11, 76:25</p> <p>forward [1] - 118:22</p> <p>four [24] - 3:11, 6:6, 9:25, 17:3, 17:5, 32:7, 45:11, 61:22, 61:23, 61:25, 66:9, 76:9, 77:6, 96:4, 96:7, 98:12, 98:17, 99:3, 99:4, 117:5, 117:20, 118:6, 118:7, 120:18</p> <p>four-part [2] - 17:3, 17:5</p> <p>framed [3] - 105:9, 106:7, 106:15</p> <p>framework [1] - 122:16</p> <p>framing [1] - 116:23</p> <p>frequently [2] - 85:23, 93:8</p> <p>friendly [5] - 63:10, 63:12, 78:4, 78:8, 98:5</p> <p>front [2] - 74:24, 85:1</p> <p>function [1] - 81:13</p> <p>functioned [2] - 50:22, 74:1</p> <p>functions [2] - 80:7, 86:10</p> <p>fundamental [5] - 45:13, 45:15, 45:18, 52:4, 90:4</p> <p>fundamentally [3] - 45:1, 45:19, 113:18</p> <p>future [1] - 76:7</p> <p style="text-align: center;">G</p> <p>gain [1] - 57:20</p> <p>gather [1] - 60:16</p> <p>gathering [1] - 101:2</p> <p>gauge [1] - 105:7</p> <p>gauging [1] - 105:5</p> <p>general [2] - 27:21, 57:1</p> <p>generally [8] - 18:7,</p>	<p>28:22, 35:2, 63:15, 90:3, 94:24, 96:11, 97:8</p> <p>generate [18] - 15:24, 16:15, 24:18, 27:23, 28:2, 28:7, 28:8, 32:3, 61:18, 63:17, 65:2, 65:24, 66:1, 66:4, 68:15, 68:16, 80:2, 120:20</p> <p>generated [23] - 15:4, 27:14, 27:15, 27:19, 28:10, 29:7, 32:13, 34:18, 62:20, 64:25, 69:3, 75:24, 76:5, 76:14, 80:4, 80:20, 89:23, 94:3, 95:2, 95:6, 96:22, 103:6, 110:4</p> <p>generates [8] - 17:23, 18:20, 29:17, 29:24, 32:1, 97:5, 102:17, 107:5</p> <p>generating [3] - 28:12, 80:5, 121:13</p> <p>generator [1] - 78:21</p> <p>generic [1] - 14:2</p> <p>gentleman [1] - 4:6</p> <p>given [28] - 8:23, 11:18, 22:22, 23:13, 31:24, 33:24, 34:16, 37:10, 38:6, 38:24, 39:15, 40:15, 40:17, 40:19, 41:19, 44:17, 60:13, 61:20, 64:3, 65:12, 66:21, 68:20, 74:17, 85:15, 96:7, 108:16, 112:16, 120:21</p> <p>gleaned [1] - 5:1</p> <p>glitch [2] - 80:19, 80:23</p> <p>goofy [1] - 116:23</p> <p>GOVERNMENT [2] - 1:11, 113:6</p> <p>government [104] - 4:11, 4:25, 6:22, 7:3, 7:18, 7:23, 8:6, 8:19, 9:6, 9:12, 9:15, 9:16, 9:21, 9:24, 9:25, 10:4, 11:2, 11:3, 11:9, 11:12, 12:18, 12:21, 13:1, 13:13, 13:19, 13:24, 14:4, 14:6, 14:16, 15:10, 15:16, 15:17, 16:4, 16:11, 16:13, 18:18, 18:22, 22:16, 24:12, 24:13, 26:8, 26:20, 29:1, 29:3, 29:7,</p>
---	---	---	---	---

30:17, 30:18, 30:21,
30:22, 31:14, 31:19,
34:14, 36:1, 40:20,
40:25, 41:2, 53:21,
61:14, 63:13, 65:5,
72:11, 72:14, 72:25,
73:9, 73:14, 73:15,
73:25, 74:5, 74:10,
74:11, 75:3, 75:19,
75:20, 77:11, 79:23,
81:20, 81:24, 85:21,
94:5, 94:14, 94:19,
95:12, 95:14, 98:1,
98:23, 99:16,
101:20, 103:21,
104:17, 104:19,
107:23, 108:2,
108:6, 108:14,
109:15, 109:18,
117:7, 117:18,
117:20, 119:4,
120:23, 121:12,
122:14

Government [1] - 2:18
government's [21] -
5:3, 6:11, 6:19, 7:15,
7:20, 8:3, 9:18,
11:14, 11:17, 13:22,
30:9, 31:17, 40:9,
57:16, 60:6, 98:19,
100:17, 101:9,
102:7, 104:1, 105:1
GOVERNMENT'S [1] -
2:12
grab [1] - 107:5
grad [1] - 21:14
graduated [1] - 20:25
ground [2] - 17:11,
121:6
grouping [1] - 17:5
groups [1] - 56:17
guess [12] - 16:9,
29:1, 36:2, 36:21,
53:7, 55:25, 56:2,
61:20, 94:17,
108:12, 111:13,
116:6
gun [1] - 100:22

H

hack [1] - 83:5
hacker [1] - 83:7
hackers [1] - 56:16
hacking [5] - 46:8,
46:12, 55:22, 55:23,
116:1
half [1] - 21:15
hand [8] - 19:21,
19:23, 31:5, 70:2,

72:9, 80:21, 100:12
handful [1] - 92:22
hard [1] - 118:1
harvested [2] - 14:10,
16:7
hat [1] - 22:10
Hayden [3] - 1:23,
124:3, 124:17
head [1] - 92:8
headquarters [2] -
42:23, 70:12
hear [3] - 26:10, 89:8,
121:19
heard [3] - 53:23,
77:12, 115:9
hearing [20] - 3:9,
4:12, 5:17, 7:17,
7:21, 10:20, 17:12,
36:3, 70:23, 71:3,
71:18, 77:16, 84:4,
88:15, 98:11, 103:8,
117:4, 120:8,
120:17, 122:18

HEARING [2] - 1:8,
2:2

hedging [1] - 113:22
held [1] - 124:8
help [2] - 41:8, 58:16
helped [1] - 45:7
helpful [23] - 6:2,
19:12, 43:21, 53:11,
63:9, 68:6, 68:9,
68:18, 68:25, 100:4,
100:5, 101:1, 102:9,
102:11, 102:14,
103:24, 103:25,
104:8, 104:11,
105:25, 111:15,
116:9, 116:10

helps [1] - 64:14
hereby [1] - 124:5
hidden [2] - 23:17,
84:5
high [4] - 61:23, 77:6,
78:19, 106:14
high-level [1] - 78:19
higher [6] - 77:22,
78:7, 85:10, 89:1,
109:16, 114:18

highly [1] - 53:5
himself [1] - 115:7
history [3] - 21:11,
21:25, 22:1
History [1] - 2:6
hit [1] - 74:23
hmm [1] - 29:18
hole [1] - 114:3
home [1] - 21:13
honest [1] - 102:5
Honor [53] - 4:17,

4:18, 11:24, 14:15,
19:3, 19:7, 19:15,
51:3, 67:3, 69:12,
69:21, 70:6, 86:16,
88:15, 89:22, 90:20,
95:16, 95:19, 95:25,
96:10, 98:11, 98:20,
99:5, 99:10, 99:12,
99:15, 99:18, 99:20,
99:25, 101:25,
102:19, 103:7,
104:3, 104:13,
107:1, 108:22,
109:21, 109:24,
110:24, 111:24,
113:1, 113:5, 113:7,
115:25, 117:4,
118:10, 118:12,
118:15, 119:9,
120:12, 121:9,
122:23, 122:25

HONORABLE [1] - 1:9

hoping [1] - 17:8

hosted [1] - 85:20

hostname [1] - 7:9

house [4] - 79:9,
79:10, 79:12, 79:15

human [13] - 23:19,
31:1, 31:11, 33:19,
63:15, 63:20, 63:25,
64:5, 64:9, 64:13,
65:14, 93:22, 98:3

human-made [1] -
33:19

human-readable [9] -
23:19, 31:11, 63:15,
63:20, 64:5, 64:9,
64:13, 65:14, 98:3

humans [5] - 32:23,
33:5, 39:9, 63:24

hundreds [3] - 71:11,
71:12, 71:15

hypothetical [2] -
56:21, 105:6

I

i.e [1] - 13:14
ID [4] - 77:3, 103:5,
107:5, 107:7

idea [2] - 52:23,
120:25

identical [1] - 49:10

identification [1] -
107:6

identified [5] - 15:12,
29:16, 50:23, 99:3,
116:17

identifier [49] - 7:6,
14:19, 14:20, 14:24,

15:5, 15:25, 16:1,
16:15, 18:21, 27:13,
27:15, 27:23, 27:25,
28:2, 28:10, 28:12,
29:5, 29:17, 32:2,
33:20, 41:5, 61:13,
61:19, 76:3, 76:10,
76:13, 76:16, 76:18,
76:21, 76:24, 77:2,
77:3, 77:7, 78:21,
80:3, 89:24, 94:2,
94:9, 94:11, 94:14,
94:18, 96:23, 103:4,
103:12, 108:17,
118:25, 121:14,
122:3

identifiers [22] -
24:19, 27:22, 29:25,
32:4, 34:17, 62:8,
62:16, 69:4, 69:7,
75:24, 76:1, 76:5,
77:4, 80:4, 80:5,
80:22, 97:6, 100:18,
102:17, 103:16,
108:20

identify [5] - 12:5,
19:4, 41:12, 48:19,
116:13

identifying [6] - 7:4,
7:11, 97:2, 110:4,
120:20, 121:14

identity [1] - 50:13

IDs [1] - 33:21

ifs [2] - 114:6, 115:2

ignoring [1] - 115:23

illegal [5] - 55:12,
85:22, 85:23, 86:23,
87:11

image [1] - 60:20

images [13] - 9:22,
14:7, 61:1, 61:16,
73:16, 99:1, 99:2,
99:3, 117:19,
117:21, 118:5,
118:7, 118:8

imaginary [1] - 56:21

immediately [1] - 78:5

impact [1] - 62:14

impeachment [1] -
101:2

important [5] - 15:2,
71:17, 73:6, 81:23,
93:14

importantly [4] - 7:19,
72:17, 80:9, 93:4

improper [1] - 41:11

improperly [1] - 75:1

in-camera [1] - 122:19

inaccurately [2] -
103:22, 104:1

inadvertently [1] -
34:6

inappropriate [2] -
105:21, 106:4

inappropriately [1] -
103:15

incident [2] - 8:18,
14:10

include [11] - 5:10,
12:6, 13:10, 13:11,
13:12, 18:19, 24:4,
24:18, 25:18, 26:7,
31:23

included [2] - 7:5,
24:17

includes [1] - 18:2

including [2] - 5:6, 7:8

incorporate [3] - 3:19,
28:3, 117:3

incorporates [1] -
30:3

incorrect [3] - 32:8,
32:10, 49:24

incorrectly [1] - 107:9

increased [1] - 103:13

inculcated [2] -
102:10, 114:22

indeed [2] - 34:17,
37:13

independently [1] -
100:24

indication [1] - 47:6

indictment [5] - 3:10,
8:22, 9:4, 98:9,
117:6

individual [5] - 80:18,
83:11, 91:18,
103:16, 119:17

individuals [1] - 112:6

infection [1] - 91:20

information [106] -
3:20, 4:23, 4:24, 5:1,
5:19, 7:4, 7:7, 7:11,
7:12, 7:18, 7:22, 8:2,
8:9, 8:12, 8:13, 9:1,
9:13, 9:21, 10:8,
10:20, 11:4, 11:7,
11:22, 14:9, 14:12,
14:22, 14:25, 15:6,
15:11, 16:4, 16:5,
16:18, 17:5, 18:24,
22:19, 23:9, 24:25,
26:11, 28:4, 28:25,
29:5, 30:11, 30:18,
30:23, 31:9, 31:13,
31:16, 31:20, 32:4,
32:5, 32:10, 39:6,
40:18, 41:1, 41:12,
48:14, 49:3, 49:24,
49:25, 52:1, 53:9,

<p>53:11, 53:21, 54:13, 54:15, 56:9, 56:12, 56:13, 57:6, 58:13, 58:25, 59:16, 59:22, 62:10, 66:1, 66:2, 66:3, 66:7, 69:5, 72:6, 73:13, 73:19, 73:23, 75:25, 89:3, 95:3, 97:3, 97:10, 97:12, 101:16, 101:19, 101:23, 102:9, 103:3, 105:11, 107:21, 108:8, 110:1, 112:9, 115:20, 120:11, 122:1, 122:4, 122:20</p> <p>information's [1] - 115:17</p> <p>informed [1] - 112:14</p> <p>inherently [2] - 51:21, 66:7</p> <p>initial [1] - 9:3</p> <p>inject [1] - 80:2</p> <p>injected [1] - 76:14</p> <p>injects [1] - 32:2</p> <p>innocent [1] - 100:21</p> <p>inquire [2] - 42:4, 70:5</p> <p>inquiring [1] - 115:25</p> <p>inserted [1] - 34:7</p> <p>inside [4] - 39:14, 46:20, 46:23, 105:9</p> <p>install [1] - 92:20</p> <p>installation [1] - 92:17</p> <p>installed [1] - 92:25</p> <p>instructions [11] - 6:15, 6:25, 7:2, 9:10, 9:19, 10:16, 12:25, 17:18, 18:9, 30:25, 73:17</p> <p>intend [1] - 4:11</p> <p>intended [8] - 45:24, 74:1, 74:6, 92:19, 93:1, 102:22, 112:22, 120:1</p> <p>intends [1] - 117:7</p> <p>intent [2] - 3:15, 121:25</p> <p>intentional [3] - 7:25, 71:16, 76:4</p> <p>intentionally [1] - 75:2</p> <p>intercept [1] - 83:25</p> <p>Internet [14] - 3:15, 7:24, 8:1, 8:7, 24:15, 25:2, 30:11, 35:16, 48:12, 56:6, 58:8, 58:9, 58:11, 72:23</p> <p>interrupt [1] - 12:12</p> <p>interruption [1] - 62:23</p> <p>interstate [1] - 42:13</p>	<p>interview [1] - 8:18</p> <p>intrusion [3] - 93:7, 93:8, 93:16</p> <p>inventory [1] - 21:18</p> <p>Investigation [1] - 70:17</p> <p>investigation [5] - 4:13, 50:22, 70:20, 93:24, 96:17</p> <p>investigative [2] - 6:13, 11:15</p> <p>Investigative [1] - 70:13</p> <p>investigators [2] - 45:10, 46:7</p> <p>involved [6] - 43:7, 43:12, 45:6, 82:20, 82:21, 82:23</p> <p>involves [2] - 3:25, 4:14</p> <p>involving [6] - 3:11, 3:12, 3:13, 3:14, 81:9, 82:4</p> <p>IP [21] - 8:4, 8:9, 8:12, 9:14, 25:2, 31:17, 39:19, 39:25, 48:6, 49:14, 50:8, 72:24, 76:18, 76:19, 93:10, 106:17, 106:22, 107:8, 107:11, 116:14, 116:15</p> <p>ISP [1] - 8:8</p> <p>issue [16] - 10:20, 33:3, 57:15, 57:19, 70:20, 71:17, 72:1, 77:4, 77:9, 77:12, 99:22, 109:23, 114:4, 115:24, 118:21, 121:8</p> <p>issued [3] - 44:21, 81:1, 113:17</p> <p>issues [5] - 11:19, 48:3, 112:3, 112:19, 121:6</p> <p>item [2] - 75:14, 75:22</p> <p>itemized [1] - 7:4</p> <p>items [4] - 72:23, 79:15, 81:25, 107:17</p> <p>itself [3] - 10:22, 85:22, 103:1</p>	<p>60:7, 61:14, 72:8, 74:16, 80:18, 82:4, 82:21, 88:11, 91:15, 104:15, 105:9, 106:7, 106:18, 116:4, 116:24, 116:25</p> <p>Jean's [44] - 4:13, 7:22, 8:13, 8:14, 8:23, 9:1, 9:3, 9:10, 9:13, 9:18, 9:19, 10:1, 10:17, 11:5, 11:11, 13:14, 13:21, 13:24, 13:25, 14:4, 18:19, 25:8, 26:3, 26:5, 43:4, 52:21, 53:2, 53:4, 53:18, 53:20, 53:25, 56:4, 60:12, 73:5, 73:9, 73:12, 73:19, 74:5, 79:24, 90:22, 95:15, 104:5, 112:2</p> <p>job [2] - 38:11, 64:20</p> <p>Joe [1] - 3:4</p> <p>joe_alfaro@fd.org [1] - 1:20</p> <p>Jose [1] - 1:17</p> <p>judge [8] - 15:13, 69:16, 89:8, 90:12, 100:2, 106:24, 110:11, 119:14</p> <p>Judge [18] - 12:23, 17:2, 18:4, 42:2, 42:4, 52:10, 68:2, 100:16, 101:7, 102:14, 105:20, 107:25, 110:7, 111:3, 111:10, 111:13, 112:4, 112:17</p> <p>judged [1] - 107:20</p> <p>Judicial [1] - 124:11</p> <p>July [3] - 91:3, 117:24, 118:2</p> <p>June [1] - 3:10</p> <p>jury [2] - 100:8, 103:23</p> <p>justify [2] - 89:19, 122:13</p>	<p>85:4</p> <p>knowledge [6] - 31:19, 34:20, 43:10, 57:22, 84:25, 96:25</p> <p>knowledgeable [1] - 55:21</p> <p>known [6] - 8:8, 9:8, 9:23, 10:19, 11:12, 82:10</p> <p>knows [3] - 12:19, 28:16, 84:10</p>	<p>letters [1] - 5:7</p> <p>level [15] - 23:5, 43:18, 64:8, 65:25, 66:5, 66:6, 68:22, 77:19, 77:22, 78:7, 78:19, 89:15, 109:16, 121:16</p> <p>leveraged [1] - 55:2</p> <p>libraries [1] - 80:7</p> <p>likelihood [1] - 120:1</p> <p>likely [12] - 57:24, 60:1, 60:14, 84:25, 87:2, 87:3, 87:23, 100:9, 116:2, 116:5, 116:7, 120:4</p> <p>limit [2] - 119:15, 120:4</p> <p>limited [1] - 121:1</p> <p>line [2] - 83:8, 107:17</p> <p>lined [3] - 17:9, 55:8, 57:22</p> <p>lines [1] - 33:1</p> <p>link [2] - 15:6, 103:15</p> <p>linkage [1] - 107:15</p> <p>linked [3] - 39:20, 106:18, 107:10</p> <p>Linux [7] - 44:13, 44:14, 52:15, 91:14, 92:3, 92:4</p> <p>listen [1] - 69:17</p> <p>listening [3] - 93:9, 93:18, 104:23</p> <p>litigation [1] - 66:15</p> <p>live [2] - 4:16, 5:12</p> <p>local [1] - 84:19</p> <p>located [2] - 43:5, 70:14</p> <p>location [1] - 35:20</p> <p>lock [7] - 54:14, 79:10, 79:13, 79:14, 107:23, 108:25</p> <p>locked [3] - 10:15, 13:6, 53:19</p> <p>log [9] - 24:19, 29:4, 29:5, 32:4, 40:18, 57:6, 58:24, 61:23, 61:24</p> <p>logged [20] - 6:17, 6:20, 24:25, 39:5, 39:19, 39:23, 39:25, 41:2, 41:12, 49:2, 49:4, 49:23, 69:4, 94:3, 96:1, 107:9, 108:15, 108:18</p> <p>logging [6] - 24:20, 30:10, 32:5, 32:11, 34:18, 56:9</p> <p>logical [1] - 120:10</p> <p>login [2] - 76:12, 76:22</p>
	<p style="text-align: center;">J</p> <p>Java [3] - 63:22, 77:24, 98:5</p> <p>JEAN [1] - 1:6</p> <p>Jean [28] - 3:2, 3:5, 3:6, 3:9, 8:20, 9:24, 12:5, 19:4, 50:14, 50:16, 50:20, 50:23,</p>	<p style="text-align: center;">K</p> <p>Kansas [1] - 21:1</p> <p>Kearney [5] - 20:10, 20:15, 20:24, 42:12, 42:15</p> <p>kind [7] - 17:10, 17:24, 23:6, 38:23, 89:5, 116:11, 116:22</p> <p>knock [1] - 116:16</p> <p>knowing [2] - 85:3,</p>	<p style="text-align: center;">L</p> <p>labels [1] - 66:3</p> <p>lack [1] - 57:16</p> <p>laid [2] - 23:14, 75:11</p> <p>language [21] - 58:21, 63:19, 64:1, 65:3, 65:5, 65:20, 68:19, 77:18, 77:20, 78:10, 78:11, 78:14, 97:16, 97:18, 97:22, 109:13, 109:14, 122:10</p> <p>languages [7] - 63:22, 63:23, 65:11, 65:14, 65:17, 77:23, 77:25</p> <p>laptop [1] - 112:2</p> <p>largely [1] - 5:1</p> <p>last [7] - 10:20, 38:23, 42:18, 59:1, 70:10, 84:3, 89:20</p> <p>late [1] - 114:25</p> <p>law [4] - 11:13, 82:23, 100:10, 114:15</p> <p>lawyer [2] - 111:7, 111:10</p> <p>lay [1] - 12:8</p> <p>lead [3] - 50:21, 101:17, 101:23</p> <p>leading [1] - 56:1</p> <p>learn [4] - 22:10, 23:25, 24:1, 65:15</p> <p>learning [1] - 56:18</p> <p>least [4] - 6:9, 103:9, 113:9, 120:9</p> <p>leave [5] - 35:13, 44:3, 54:8, 54:10, 112:16</p> <p>led [2] - 8:13, 67:22</p> <p>left [5] - 14:13, 53:6, 54:7, 93:6, 93:15</p> <p>legal [4] - 57:17, 86:9, 86:22, 87:2</p> <p>legitimate [1] - 85:19</p> <p>legitimately [1] - 86:5</p> <p>lends [1] - 88:23</p> <p>less [7] - 51:25, 52:1, 60:13, 116:5, 116:6, 119:23, 122:4</p>	

<p>logins [1] - 76:8 logistics [1] - 122:17 logs [2] - 29:25, 59:22 look [37] - 23:14, 24:22, 26:2, 26:3, 32:21, 33:8, 37:5, 40:3, 43:21, 43:24, 43:25, 44:11, 49:20, 59:13, 61:11, 64:10, 77:25, 78:4, 79:10, 83:23, 86:7, 91:23, 92:16, 94:10, 94:13, 96:5, 100:21, 106:25, 110:14, 112:20, 112:21, 115:12, 115:13, 115:14, 116:25 looked [10] - 36:12, 36:13, 36:14, 36:16, 43:11, 49:25, 62:18, 80:3, 92:2, 92:22 looking [17] - 23:11, 23:15, 36:7, 43:25, 57:23, 58:10, 60:17, 78:14, 79:3, 79:25, 85:1, 87:6, 91:20, 93:13, 101:24, 112:23, 116:24 looks [1] - 13:9 loop [1] - 119:24 lose [2] - 66:1, 103:21 loss [1] - 31:13 lost [4] - 22:16, 23:9, 62:21, 66:7 low [4] - 23:5, 61:23, 77:7, 77:19 low-level [2] - 23:5, 77:19 lower [2] - 57:25, 65:25 lurking [1] - 56:5</p>	<p>majors [1] - 37:19 malfunctioning [1] - 104:2 malicious [1] - 55:22 maliciously [1] - 59:15 malware [2] - 24:4, 91:19 man [1] - 116:18 manage [1] - 21:18 manner [8] - 10:19, 26:24, 26:25, 34:14, 39:5, 48:21, 86:3, 87:16 Manuel [1] - 1:17 manufactured [1] - 106:16 March [4] - 90:22, 96:3, 98:13, 117:11 marks [1] - 61:9 Maryland [1] - 70:15 massive [1] - 84:23 master's [2] - 21:1, 21:5 match [10] - 16:4, 16:6, 49:16, 49:21, 50:6, 62:9, 74:20, 76:17, 79:22 matched [1] - 49:24 matches [2] - 74:24, 75:1 matching [1] - 62:8 material [24] - 3:12, 3:13, 11:5, 11:11, 18:18, 55:13, 57:19, 60:12, 75:21, 78:14, 79:14, 82:23, 97:9, 97:12, 102:19, 104:15, 105:5, 105:11, 107:18, 107:19, 107:23, 108:1, 114:17, 122:15 materiality [14] - 11:7, 61:17, 81:24, 82:7, 82:17, 96:25, 99:22, 100:3, 100:14, 100:15, 104:23, 105:19, 114:15, 122:13 Matish [6] - 26:1, 66:16, 66:17, 66:18, 66:20, 72:4 matter [15] - 3:1, 11:9, 43:7, 53:10, 53:21, 72:3, 72:9, 76:1, 80:14, 80:21, 80:24, 82:24, 105:15, 118:22, 124:9 matters [1] - 101:10 Matthew [2] - 4:7, 20:7</p>	<p>MATTHEW [2] - 2:8, 20:1 mean [13] - 7:14, 17:17, 22:20, 27:20, 35:18, 41:10, 46:24, 49:19, 81:5, 96:21, 100:21, 106:11, 107:7 means [8] - 10:9, 10:12, 10:18, 12:22, 17:14, 56:5, 77:7, 107:10 meant [1] - 71:11 measure [2] - 39:17, 97:17 measuring [1] - 89:15 media [1] - 33:9 member [5] - 80:15, 83:12, 83:19, 84:17, 87:12 memory [1] - 90:21 mention [1] - 66:13 mentioned [6] - 24:8, 43:11, 45:17, 53:13, 77:10, 77:24 mere [3] - 45:24, 47:21, 59:16 merely [2] - 105:6, 107:19 message [1] - 77:2 met [2] - 42:9, 100:2 Metasploit [1] - 35:21 method [7] - 10:9, 10:12, 31:6, 40:12, 48:2, 48:11, 94:22 methodology [2] - 44:9, 75:23 methods [3] - 37:18, 48:5, 75:17 Michaud [6] - 25:12, 44:22, 66:15, 66:20, 101:5, 102:1 micro [1] - 103:7 microphone [1] - 71:9 might [5] - 6:24, 51:20, 65:21, 115:5 MILLER [6] - 2:8, 4:9, 20:1, 121:18, 121:21, 122:7 Miller [50] - 4:7, 5:11, 11:21, 12:7, 15:1, 15:15, 15:22, 16:20, 16:23, 17:7, 17:21, 18:23, 19:8, 19:10, 19:16, 19:18, 20:5, 20:7, 20:8, 42:8, 52:14, 62:24, 67:6, 69:14, 72:18, 72:19, 74:9, 76:2, 77:1, 77:16, 77:21, 77:23,</p>	<p>79:20, 79:21, 81:15, 81:19, 90:14, 102:22, 103:2, 112:12, 119:1, 119:6, 119:8, 119:13, 119:17, 119:21, 120:10, 120:14, 121:16, 121:17 Miller's [8] - 79:5, 80:25, 83:1, 98:1, 102:2, 113:14, 115:3, 121:1 millions [1] - 33:1 mind [1] - 56:22 minor [3] - 3:13, 3:14, 98:15 Mint [1] - 92:3 minute [2] - 90:13, 106:20 minutes [1] - 90:16 mis [2] - 106:17, 107:9 miscategorized [1] - 106:17 miscategory [1] - 107:9 miss [1] - 64:22 missing [1] - 31:9 misspoke [1] - 107:2 misspoken [1] - 71:8 misstate [1] - 71:15 misstated [1] - 76:2 misstatement [2] - 71:6, 76:4 mistakes [3] - 32:24, 32:25, 33:2 modified [2] - 36:17, 69:6 modifies [3] - 26:24, 27:1, 46:21 modify [1] - 46:2 moniker [1] - 50:17 monitor [2] - 56:12 monitored [4] - 14:6, 55:11, 117:8, 117:13 monitoring [8] - 19:1, 55:9, 56:24, 56:25, 67:7, 68:4, 84:11, 84:18 monitors [1] - 95:7 months [2] - 42:12, 117:22 moreover [2] - 89:1, 112:14 most [11] - 18:5, 33:3, 65:4, 65:7, 65:13, 93:4, 93:13, 100:21, 104:24, 112:6, 120:10 motion [12] - 3:8,</p>	<p>3:22, 3:24, 3:25, 4:21, 5:2, 5:21, 11:23, 70:24, 72:2, 118:17 MOTION [2] - 1:8, 2:2 Motion [1] - 2:19 mount [1] - 115:22 Mountain [1] - 1:24 mounting [1] - 115:20 move [1] - 47:4 moving [1] - 72:1 MR [91] - 4:9, 4:17, 4:18, 11:24, 12:15, 12:23, 14:15, 15:13, 16:8, 17:2, 18:4, 18:9, 18:12, 19:3, 19:7, 19:15, 20:4, 42:2, 42:4, 42:7, 51:3, 51:6, 51:9, 52:10, 62:21, 67:3, 67:5, 67:20, 68:2, 69:9, 69:11, 69:16, 69:21, 69:24, 70:6, 70:8, 86:16, 86:19, 86:21, 88:14, 88:19, 89:8, 89:22, 90:12, 90:20, 95:16, 95:19, 99:10, 99:12, 99:18, 99:20, 99:25, 100:2, 105:20, 106:3, 106:24, 107:25, 108:9, 108:12, 108:22, 109:21, 110:7, 110:11, 110:14, 110:16, 110:24, 111:6, 111:8, 111:13, 111:22, 111:24, 112:4, 113:1, 113:5, 113:7, 115:1, 117:10, 117:16, 117:23, 118:10, 118:12, 118:15, 119:8, 119:14, 120:12, 121:9, 121:18, 121:21, 122:7, 122:23, 122:25 multiple [1] - 31:22 museum [1] - 42:13 must [1] - 49:11 mutually [1] - 5:16</p>
M				
<p>MAC [1] - 7:9 machine [5] - 1:21, 44:13, 44:14, 91:14, 93:1 machines [1] - 100:23 Mail [8] - 67:14, 68:3, 85:16, 85:22, 85:24, 85:25, 86:6, 87:18 mails [1] - 5:7 Main [1] - 37:1 main [1] - 75:5 maintained [1] - 75:20 major [1] - 47:2 Major [1] - 70:14 majority [3] - 87:14, 87:22, 88:20</p>				
N				
<p>name [7] - 20:5, 20:7, 42:8, 63:12, 70:10, 111:5 named [1] - 92:12 national [1] - 70:19</p>				

<p>nationwide [1] - 114:2 nature [4] - 86:8, 89:11, 91:20, 98:6 near [1] - 78:11 Nebraska [3] - 20:10, 20:14, 20:24 necessarily [15] - 10:5, 31:13, 35:5, 38:2, 41:15, 43:16, 44:3, 47:25, 48:1, 49:12, 62:17, 68:12, 81:17, 113:19, 117:23 necessary [6] - 5:24, 16:23, 18:24, 33:25, 89:18, 111:18 need [22] - 8:25, 11:14, 14:13, 25:14, 31:25, 32:12, 38:13, 38:25, 39:4, 69:18, 71:5, 73:24, 79:18, 84:25, 94:20, 103:3, 103:4, 104:9, 112:18, 119:11, 121:7, 122:17 needed [1] - 72:14 needing [1] - 61:17 needs [3] - 32:19, 94:3, 94:18 nefarious [7] - 53:14, 53:24, 54:21, 56:3, 56:22, 59:12, 67:7 network [14] - 6:12, 49:8, 55:6, 71:10, 71:13, 74:8, 74:13, 83:15, 84:4, 84:23, 91:21, 91:23, 93:3, 95:10 networking [1] - 91:17 networks [1] - 59:14 never [2] - 42:9, 79:11 new [4] - 28:7, 56:19, 96:13, 96:15 next [3] - 28:18, 30:12, 86:14 NIT [132] - 6:6, 6:12, 6:13, 6:23, 7:7, 7:17, 9:8, 9:18, 10:6, 10:13, 12:2, 12:6, 12:10, 12:25, 13:2, 13:7, 13:13, 13:23, 14:5, 14:17, 14:18, 15:21, 16:2, 16:11, 16:14, 16:16, 17:4, 17:6, 17:17, 18:6, 18:12, 18:15, 18:17, 19:4, 24:10, 25:8, 26:4, 26:8, 26:19, 26:21, 27:3, 27:4, 27:7, 27:12, 27:13,</p>	<p>28:3, 28:6, 28:9, 28:19, 28:24, 28:25, 30:1, 30:6, 30:7, 31:7, 31:24, 43:2, 44:2, 44:7, 44:10, 44:13, 45:13, 45:20, 45:22, 46:8, 46:18, 46:19, 47:5, 47:20, 49:5, 49:8, 52:6, 52:15, 52:19, 53:3, 53:5, 53:18, 54:7, 54:10, 54:13, 54:15, 57:5, 63:1, 63:4, 64:12, 66:18, 67:15, 67:16, 68:23, 72:11, 72:16, 72:23, 73:2, 73:5, 75:18, 76:11, 76:14, 76:17, 76:25, 77:5, 77:13, 78:6, 78:9, 79:4, 79:19, 81:17, 88:9, 88:12, 90:21, 95:8, 96:9, 96:10, 96:16, 96:19, 96:20, 97:15, 97:24, 102:8, 109:12, 112:10, 114:11, 116:12, 116:20, 116:24 NIT's [3] - 6:25, 10:15, 95:14 NIT/payload [1] - 30:22 NITs [1] - 22:7 NO [1] - 1:5 nobody [1] - 115:14 nodes [1] - 71:14 nomenclature [4] - 3:20, 6:1, 6:4, 17:11 noncustodial [1] - 8:17 none [2] - 37:7, 43:10 nonissue [1] - 80:23 normal [1] - 23:1 note [3] - 81:23, 85:14, 86:2 noted [3] - 73:20, 77:23, 111:23 notes [1] - 107:1 nothing [8] - 37:21, 73:1, 77:7, 82:8, 82:18, 94:8, 103:21 notice [1] - 93:16 noticed [1] - 36:4 noting [1] - 73:3 Nth [1] - 89:17 number [25] - 3:3, 3:23, 4:14, 9:7, 9:25, 11:3, 16:1, 16:3, 16:18, 16:19, 61:19, 61:22, 77:23, 80:20,</p>	<p>83:20, 85:9, 89:1, 95:25, 96:21, 103:9, 103:13, 110:20, 120:20, 121:14 numbers [4] - 80:6, 92:13, 97:2, 110:4 numerous [1] - 71:24</p> <p style="text-align: center;">O</p> <p>oath [2] - 19:18, 109:16 object [1] - 5:21 objection [4] - 11:6, 67:20, 88:14, 89:21 objects [1] - 10:24 observed [4] - 5:14, 72:20, 74:3, 79:22 obtain [1] - 107:21 obtained [1] - 8:11 obtaining [1] - 60:11 obviously [4] - 14:9, 59:6, 105:1, 105:3 occasions [1] - 96:9 occur [5] - 17:7, 27:10, 33:2, 33:4, 54:2 occurred [8] - 48:17, 54:6, 85:13, 114:6, 114:10, 114:11, 117:11 occurs [1] - 31:13 October [3] - 1:9, 2:5, 124:12 odds [4] - 57:12, 85:3, 85:25, 86:11 OF [4] - 1:1, 1:3, 1:8, 124:1 off-the-shelf [1] - 82:20 offense [1] - 42:15 offensive [1] - 46:10 offensive-based [1] - 46:10 Office [1] - 1:13 Official [3] - 1:23, 124:3, 124:17 OFFICIAL [1] - 124:1 often [2] - 32:25, 100:12 once [6] - 41:13, 80:20, 88:11, 96:10, 103:6 One [4] - 98:16, 99:4, 117:5, 118:7 one [78] - 3:13, 3:14, 4:12, 9:7, 10:8, 10:24, 11:3, 13:8, 17:4, 18:1, 23:5, 27:14, 27:23, 32:9,</p>	<p>34:25, 36:9, 36:21, 36:25, 37:2, 37:15, 38:11, 38:12, 40:12, 45:10, 46:7, 48:6, 49:2, 53:8, 53:12, 55:1, 57:2, 57:14, 58:18, 64:8, 65:15, 65:16, 66:5, 66:6, 67:13, 67:17, 71:9, 75:14, 76:24, 77:12, 78:7, 78:11, 78:12, 81:9, 82:4, 82:6, 86:4, 88:7, 91:25, 93:5, 93:13, 96:20, 96:21, 96:23, 97:20, 97:21, 98:12, 103:11, 107:1, 108:24, 110:1, 110:11, 110:23, 114:4, 117:10, 118:22, 120:5, 120:6 one-time [1] - 76:24 one-to-one [3] - 78:11, 78:12, 86:4 ones [3] - 36:16, 38:17, 77:25 online [2] - 21:20, 50:17 Onyx [3] - 21:15, 21:16, 21:17 open [2] - 54:8, 54:14 opened [1] - 67:24 opening [1] - 75:11 operate [1] - 103:14 operated [1] - 34:13 operating [11] - 6:25, 7:10, 9:10, 17:18, 37:12, 39:14, 39:17, 51:20, 91:15, 92:3, 95:24 operation [7] - 83:14, 83:22, 84:15, 85:4, 85:16, 88:12, 90:25 opine [1] - 50:21 opining [1] - 111:11 opinion [10] - 33:25, 68:6, 78:22, 78:25, 83:8, 87:14, 111:18, 118:18, 118:20, 122:12 opportunities [1] - 56:6 opportunity [1] - 30:16 opposed [4] - 7:24, 23:11, 46:20, 64:4 order [36] - 3:21, 3:22, 6:2, 7:5, 12:9, 13:5, 17:5, 21:19, 22:10, 22:13, 25:14, 27:12,</p>	<p>27:13, 28:13, 41:4, 55:8, 55:20, 68:15, 72:14, 73:25, 83:10, 83:17, 83:22, 84:24, 94:21, 104:17, 104:18, 119:5, 119:16, 120:2, 120:13, 121:12, 121:22, 121:24, 122:10, 122:21 ordered [3] - 47:15, 119:4, 121:20 orders [2] - 119:23, 120:4 organizer [1] - 17:24 organizers [1] - 109:9 original [2] - 23:7, 65:1 originally [1] - 78:7 originated [3] - 61:2, 62:9, 66:14 originating [1] - 96:21 OS10 [1] - 32:21 otherwise [3] - 10:6, 60:25, 120:2 outline [1] - 19:14 output [3] - 72:20, 74:3, 79:22 outside [7] - 18:15, 18:17, 21:13, 35:14, 93:7, 93:8, 93:16 over-the-Internet- based [1] - 48:12 overwritten [3] - 51:15, 52:2, 112:12 own [4] - 9:22, 85:8, 87:24, 102:13</p> <p style="text-align: center;">P</p> <p>p.m [4] - 1:9, 90:17, 123:2 packet [1] - 8:2 packets [3] - 8:4, 8:5, 8:9 page [8] - 6:7, 58:23, 58:25, 71:9, 81:12, 110:20, 110:25, 124:9 Page [2] - 2:4, 46:5 pages [1] - 14:7 paid [1] - 20:19 papers [1] - 5:10 paragraph [4] - 44:24, 110:20, 110:25, 111:2 paranoid [2] - 58:6, 58:11 paraphrase [2] - 59:24, 90:7</p>
--	--	---	--	---

<p>Parker [1] - 1:13</p> <p>part [23] - 12:6, 12:10, 17:3, 17:4, 17:5, 18:2, 18:5, 29:24, 38:11, 39:20, 46:6, 61:4, 61:11, 64:12, 76:10, 77:5, 94:25, 96:17, 97:8, 106:25, 109:22, 110:9, 118:8</p> <p>partially [1] - 64:6</p> <p>participate [1] - 69:15</p> <p>particular [10] - 4:13, 16:5, 16:7, 27:24, 31:17, 47:6, 93:9, 98:6, 109:20, 111:21</p> <p>particularly [3] - 97:6, 100:19, 102:23</p> <p>parties [4] - 5:6, 5:9, 5:16, 10:24</p> <p>parties' [1] - 5:2</p> <p>parts [2] - 17:3, 18:16</p> <p>party [7] - 35:14, 53:14, 54:20, 59:10, 60:10, 108:5, 109:5</p> <p>pass [2] - 10:13, 42:2</p> <p>passage [1] - 51:24</p> <p>passed [3] - 42:12, 51:22, 53:19</p> <p>passes [1] - 51:25</p> <p>past [2] - 21:25, 67:18</p> <p>path [3] - 36:9, 89:19, 114:24</p> <p>paths [4] - 36:10, 36:13, 38:3, 112:21</p> <p>pathways [9] - 36:19, 36:25, 37:7, 37:18, 37:20, 37:21, 38:8, 41:21</p> <p>payload [21] - 15:5, 16:10, 16:14, 17:17, 18:7, 18:9, 18:13, 18:15, 18:17, 27:8, 27:12, 27:16, 28:20, 30:6, 32:2, 52:7, 57:7, 63:2, 72:12, 72:17, 72:21</p> <p>payloads [1] - 17:13</p> <p>PCAP [13] - 29:6, 31:16, 40:1, 40:4, 43:3, 44:18, 49:3, 66:24, 74:7, 95:3, 95:6, 95:11, 95:13</p> <p>penetration [1] - 24:5</p> <p>people [31] - 35:22, 45:6, 56:5, 56:8, 56:11, 56:14, 56:15, 56:19, 58:4, 58:5, 59:3, 59:4, 59:13, 59:14, 59:23, 67:6, 87:4, 88:1, 88:2,</p>	<p>88:3, 88:5, 88:9, 88:20, 88:22, 88:24, 89:12, 93:12, 119:23, 119:24</p> <p>percent [2] - 50:4, 113:24</p> <p>perfect [1] - 71:21</p> <p>performs [1] - 91:19</p> <p>perhaps [1] - 58:17</p> <p>period [4] - 95:23, 96:2, 112:13, 117:14</p> <p>permanent [1] - 26:25</p> <p>permanently [1] - 46:3</p> <p>permission [2] - 120:13, 122:5</p> <p>person [15] - 23:1, 50:7, 50:10, 53:1, 55:7, 56:2, 56:21, 57:22, 80:16, 108:16, 114:4, 116:17, 120:10</p> <p>pertain [1] - 98:17</p> <p>pertaining [1] - 72:3</p> <p>Ph.D [1] - 21:7</p> <p>phone [1] - 32:22</p> <p>physical [2] - 40:19, 79:8</p> <p>pick [7] - 54:14, 65:15, 79:10, 79:11, 79:13, 79:14, 108:25</p> <p>picked [1] - 107:23</p> <p>pictures [1] - 79:16</p> <p>piece [13] - 10:8, 10:23, 10:25, 16:12, 22:22, 26:22, 36:8, 37:18, 40:7, 72:13, 81:8, 91:21, 97:11</p> <p>pieces [7] - 7:4, 7:12, 8:25, 15:11, 16:3, 73:23, 110:1</p> <p>place [4] - 14:2, 39:18, 57:23, 117:7</p> <p>Plaintiff [1] - 1:4</p> <p>plan [1] - 102:12</p> <p>planned [1] - 35:5</p> <p>play [1] - 48:3</p> <p>Playpen [40] - 6:18, 10:11, 14:8, 19:1, 25:7, 39:4, 43:8, 50:7, 56:24, 60:9, 61:16, 66:15, 70:19, 80:15, 82:21, 82:24, 83:6, 83:13, 83:16, 83:19, 84:6, 84:10, 84:12, 84:17, 86:3, 86:9, 86:14, 87:15, 87:19, 87:21, 87:22, 88:13, 95:23, 96:8, 96:17, 96:20, 98:18, 98:23, 114:2, 117:8</p>	<p>plea [2] - 101:17, 102:13</p> <p>plow [1] - 114:23</p> <p>plus [1] - 121:16</p> <p>point [19] - 9:7, 27:23, 44:4, 50:18, 55:1, 60:3, 60:4, 78:2, 78:6, 89:18, 101:6, 105:5, 110:5, 110:20, 111:1, 111:20, 111:22, 115:2, 116:6</p> <p>population [1] - 58:11</p> <p>pornography [16] - 3:16, 6:18, 6:23, 8:21, 9:11, 60:8, 73:16, 84:22, 86:10, 87:13, 98:17, 98:22, 108:13, 109:6, 116:13, 118:1</p> <p>port [1] - 93:9</p> <p>portion [2] - 5:20, 47:23</p> <p>ports [2] - 93:10, 93:13</p> <p>position [10] - 11:10, 21:9, 59:11, 60:18, 60:23, 61:1, 75:21, 101:20, 105:18, 122:2</p> <p>possessing [1] - 3:13</p> <p>possession [4] - 18:18, 99:1, 117:17, 117:23</p> <p>possibilities [10] - 35:7, 38:14, 41:14, 48:17, 53:12, 57:3, 64:22, 102:20, 106:18, 114:6</p> <p>possibility [15] - 32:9, 33:16, 39:8, 46:2, 51:11, 54:7, 57:11, 57:13, 62:15, 74:25, 85:11, 105:14, 106:21, 111:14, 119:20</p> <p>possible [22] - 33:20, 33:23, 34:4, 34:9, 34:19, 36:12, 37:25, 41:21, 51:22, 57:25, 58:1, 62:19, 88:21, 90:4, 93:21, 96:15, 104:4, 107:14, 112:15, 115:8, 118:18, 120:25</p> <p>possibly [4] - 38:19, 83:5, 111:15, 115:22</p> <p>posture [1] - 4:22</p> <p>potential [1] - 111:11</p> <p>potentiality [1] - 57:18</p>	<p>potentially [4] - 54:20, 56:3, 108:12, 122:1</p> <p>precaution [1] - 53:10</p> <p>precise [2] - 56:25, 121:24</p> <p>precludes [1] - 84:9</p> <p>preparation [1] - 101:4</p> <p>prepare [1] - 45:7</p> <p>prepared [2] - 56:4, 121:9</p> <p>preparedness [1] - 55:7</p> <p>preparing [4] - 93:23, 100:4, 104:16, 105:25</p> <p>present [10] - 4:22, 54:5, 83:1, 89:2, 98:10, 100:7, 103:23, 105:23, 112:10, 113:11</p> <p>presented [1] - 11:19</p> <p>preserving [1] - 55:9</p> <p>prevent [1] - 11:14</p> <p>previous [3] - 36:2, 79:1, 84:4</p> <p>previously [7] - 36:1, 38:23, 53:17, 70:22, 71:2, 73:20, 94:16</p> <p>prime [1] - 58:5</p> <p>privilege [2] - 11:13, 11:17</p> <p>proactive [2] - 55:10, 57:5</p> <p>probability [2] - 104:2, 106:15</p> <p>probable [1] - 57:24</p> <p>Procedural [1] - 2:6</p> <p>proceed [2] - 19:14, 69:23</p> <p>proceeding [3] - 3:1, 3:8, 4:20</p> <p>proceedings [4] - 47:20, 62:23, 123:2, 124:8</p> <p>Proceedings [1] - 1:21</p> <p>process [10] - 27:11, 30:13, 31:10, 38:24, 66:1, 78:2, 80:6, 94:22, 94:25, 112:11</p> <p>produce [2] - 11:2, 119:4</p> <p>produced [5] - 5:21, 9:7, 9:16, 13:13, 44:16</p> <p>producing [1] - 63:14</p> <p>product [1] - 21:20</p> <p>professor [2] - 20:9, 21:10</p>	<p>proffer [2] - 103:25, 106:12</p> <p>program [5] - 22:12, 31:1, 66:8, 78:13, 95:12</p> <p>programmed [2] - 21:17, 32:23</p> <p>programmer [4] - 21:14, 21:23, 21:24, 58:20</p> <p>programmer's [1] - 58:21</p> <p>programming [9] - 28:15, 33:5, 38:10, 65:3, 65:13, 65:20, 77:19, 77:22, 80:6</p> <p>programs [5] - 18:16, 22:11, 23:25, 33:10, 92:14</p> <p>prompt [3] - 67:1, 95:18, 99:9</p> <p>pronounce [1] - 111:4</p> <p>proper [3] - 4:3, 48:21, 69:5</p> <p>properly [6] - 25:15, 32:11, 39:20, 39:25, 50:22, 80:9</p> <p>prosecuted [1] - 114:1</p> <p>prosecutor [1] - 43:14</p> <p>protect [1] - 56:10</p> <p>protections [2] - 82:13, 82:14</p> <p>protective [6] - 119:5, 119:23, 120:2, 121:12, 121:24, 122:10</p> <p>prove [6] - 101:22, 104:9, 104:10, 105:1, 105:2, 117:7</p> <p>proved [2] - 101:11, 101:12</p> <p>provide [7] - 4:25, 25:6, 65:5, 65:6, 66:12, 97:9, 109:18</p> <p>provided [40] - 4:24, 7:20, 13:20, 17:25, 26:18, 27:5, 30:17, 30:18, 30:21, 30:22, 31:14, 31:15, 31:19, 40:22, 40:25, 49:9, 50:18, 63:1, 63:6, 63:9, 64:4, 65:8, 66:24, 68:24, 72:7, 72:10, 72:17, 74:9, 74:16, 74:24, 75:25, 78:15, 79:1, 79:17, 79:19, 79:23, 97:15, 109:17, 113:15, 121:15</p> <p>provider [1] - 8:8</p>
---	--	---	--	--

<p>provides [1] - 47:15 providing [3] - 57:16, 64:18, 64:19 proving [1] - 117:19 proxies [1] - 48:5 proxy [5] - 46:23, 84:1, 84:2, 84:19, 85:6 Public [1] - 1:18 public [1] - 88:6 published [1] - 82:10 pull [1] - 66:5 pulling [1] - 23:5 purpose [10] - 17:9, 50:10, 59:11, 76:3, 76:6, 76:13, 79:15, 80:8, 80:14, 87:11 purposes [9] - 3:18, 50:5, 56:22, 67:7, 85:9, 85:23, 87:25, 89:7, 117:4 pursuant [2] - 10:2, 124:6 pursue [1] - 106:6 pursuing [1] - 106:8 push [1] - 116:11 pushed [1] - 118:22 put [13] - 5:16, 5:24, 14:24, 27:16, 29:25, 39:23, 60:5, 64:16, 101:25, 105:18, 113:9, 113:13, 121:22 putting [3] - 60:12, 101:6, 101:21</p>	<p>39:3, 44:2, 44:3, 44:13, 45:24, 46:21, 46:22, 52:25, 53:20, 66:22, 90:21, 91:8 randomly [1] - 103:14 rank [1] - 59:25 rather [3] - 43:18, 81:18, 109:13 raw [6] - 49:8, 74:10, 74:14, 74:15, 74:18, 95:13 RC.D [2] - 92:12 re [1] - 29:23 re-explain [1] - 29:23 reach [1] - 72:22 reaches [1] - 73:9 read [12] - 17:15, 23:2, 23:19, 47:22, 62:3, 64:7, 64:9, 71:3, 78:1, 81:2, 98:10 readable [9] - 23:19, 31:11, 63:15, 63:20, 64:5, 64:9, 64:13, 65:14, 98:3 reader [2] - 63:10, 63:12 reader-friendly [2] - 63:10, 63:12 reading [3] - 5:14, 66:10, 71:4 ready [1] - 16:13 real [5] - 50:7, 50:10, 50:13, 71:17, 80:16 realistically [2] - 58:1, 84:24 realize [2] - 58:4, 58:8 really [11] - 10:8, 37:4, 46:16, 57:18, 61:5, 65:16, 67:23, 85:2, 89:18, 93:13, 106:14 Realtime [1] - 124:3 realtime [1] - 1:21 reason [5] - 39:2, 52:19, 97:1, 115:19, 119:10 reasonable [4] - 103:25, 104:2, 104:9, 104:10 reasonably [3] - 65:5, 65:6, 106:14 reasons [3] - 56:8, 89:19, 104:14 reboots [1] - 51:16 rebuttal [4] - 69:18, 99:19, 99:20, 101:3 receipt [3] - 3:12, 117:6, 117:20 receipts [1] - 117:7 received [15] - 8:10, 18:3, 18:5, 18:23,</p>	<p>19:4, 19:9, 30:11, 41:2, 54:25, 95:8, 95:12, 95:13, 98:13, 107:13, 109:23 receiving [1] - 29:4 receives [2] - 14:22, 15:7 recently [1] - 77:16 recess [3] - 90:13, 90:16, 90:17 recollection [1] - 91:3 record [2] - 20:6, 117:2 recorded [1] - 1:21 red [1] - 56:16 REDIRECT [2] - 51:8, 67:4 Redirect [2] - 2:10, 2:11 REDIRECT-EXAMINATION [1] - 67:4 reduced [1] - 120:17 reducing [1] - 119:25 refer [7] - 9:7, 10:25, 17:19, 18:7, 27:8, 81:4, 107:3 reference [2] - 3:19, 98:12 referenced [1] - 79:2 references [1] - 67:13 referred [11] - 9:17, 18:20, 72:10, 72:11, 72:15, 74:13, 77:3, 77:19, 81:4, 85:15, 112:12 referring [4] - 36:19, 68:19, 91:8, 94:15 refine [1] - 121:12 reflect [1] - 117:25 reflects [1] - 74:18 refuses [1] - 11:2 regalbegal [26] - 6:21, 6:22, 9:23, 10:11, 14:8, 32:6, 50:14, 50:17, 50:21, 50:23, 60:7, 61:15, 76:8, 76:16, 76:18, 76:20, 95:22, 96:8, 96:24, 108:15, 116:5, 116:16, 116:17, 116:19, 117:8 regalbegal's [11] - 6:25, 7:8, 7:10, 8:3, 8:4, 8:10, 8:12, 13:14, 16:2, 19:1, 96:19 regard [2] - 8:24, 109:8 regarding [10] - 26:11,</p>	<p>33:18, 35:25, 38:22, 70:23, 72:8, 103:3, 110:17, 112:6, 114:2 regards [4] - 27:11, 88:21, 102:16, 110:16 regular [8] - 7:23, 8:1, 25:2, 30:11, 32:22, 58:8, 58:9, 58:11 regulations [1] - 124:10 reintroduce [1] - 70:9 related [2] - 10:5, 43:1 relates [1] - 118:24 relationship [1] - 78:12 relatively [2] - 60:10, 88:8 relativity [1] - 60:10 released [2] - 67:16, 88:7 relevant [8] - 21:25, 67:21, 88:16, 88:19, 89:3, 102:11, 105:24 reliability [1] - 47:7 reliable [3] - 47:14, 48:2, 52:1 relied [1] - 97:8 rely [1] - 107:22 remain [1] - 69:17 remained [3] - 52:20, 52:23, 53:3 remaining [1] - 8:24 remains [1] - 94:8 remember [7] - 46:13, 47:8, 54:11, 67:8, 90:24, 92:8, 92:9 remnants [4] - 53:3, 53:5, 54:8, 54:10 remote [4] - 35:17, 35:20, 35:23, 105:13 remotely [1] - 34:10 removed [2] - 51:19, 52:24 render [2] - 102:12, 104:5 rendered [1] - 109:4 rephrase [1] - 29:14 report [14] - 45:8, 46:4, 46:6, 47:13, 48:10, 64:10, 74:17, 81:1, 81:11, 81:13, 81:19, 90:25, 96:5 REPORTED [1] - 124:8 REPORTER [1] - 124:1 Reporter [3] - 1:23, 124:4, 124:17 Reporter's [1] - 2:21 representation [2] -</p>	<p>31:3, 77:18 represented [2] - 13:1, 47:24 representing [1] - 88:20 represents [1] - 34:14 reproduced [1] - 49:11 request [4] - 78:17, 104:17, 113:23, 119:16 requested [3] - 24:23, 81:22, 104:19 requesting [9] - 11:25, 12:2, 12:4, 15:3, 26:12, 75:10, 75:14, 78:20, 109:22 requests [2] - 75:12, 101:10 require [1] - 46:9 required [3] - 26:19, 31:23, 102:7 reread [1] - 17:15 researcher [2] - 86:6, 87:12 researchers [1] - 87:3 residential [2] - 10:3, 14:10 resolve [2] - 109:20, 109:23 respect [3] - 96:19, 97:5, 97:23 respectfully [2] - 105:21, 119:16 respond [2] - 73:17, 105:20 response [6] - 5:4, 36:5, 36:6, 73:15, 101:9, 112:4 responsible [2] - 76:11, 121:13 restrictions [1] - 122:11 result [7] - 73:5, 92:19, 92:25, 95:14, 98:22, 100:9, 104:11 resulted [2] - 73:4, 109:5 results [4] - 16:6, 52:17, 76:17, 120:14 retained [3] - 24:8, 24:9, 66:13 retool [1] - 87:24 retransmission [1] - 47:16 returned [3] - 16:3, 53:20, 106:23 reuse [2] - 27:24, 85:8 reveal [5] - 25:2, 37:24, 38:2, 38:3,</p>
Q				
<p>questions [7] - 51:6, 52:10, 53:9, 57:14, 90:19, 99:7, 104:20 quickly [2] - 65:16, 118:20 quote [1] - 90:7 quote/unquote [4] - 8:2, 10:14, 11:11, 13:9 quoted [1] - 71:10 quoting [3] - 44:25, 46:5, 48:10</p>				
R				
<p>radar [1] - 100:22 raise [3] - 19:20, 19:22, 70:2 raised [1] - 57:15 ran [20] - 7:2, 9:19, 13:2, 13:5, 14:5, 24:24, 28:4, 28:6,</p>				

<p>122:14 reverse [14] - 22:3, 22:5, 22:11, 22:15, 22:17, 22:20, 23:4, 23:10, 23:18, 24:5, 27:5, 37:6, 38:5, 68:21 review [10] - 25:6, 26:17, 30:16, 68:25, 69:2, 93:19, 93:20, 103:4, 103:5, 109:12 reviewed [10] - 25:17, 25:21, 26:5, 42:25, 43:2, 43:5, 71:1, 91:9, 102:18, 102:25 reviewing [2] - 102:8, 106:13 rewritable [1] - 51:21 rid [1] - 40:20 risk [2] - 89:2, 103:13 RMR [2] - 1:23, 124:17 Rock [2] - 42:23, 115:13 Rule [2] - 11:4, 100:14 rule [2] - 53:11, 121:5 ruling [1] - 57:18 run [35] - 10:16, 13:7, 13:14, 13:17, 16:2, 18:17, 25:16, 26:23, 27:2, 28:25, 30:25, 34:4, 35:4, 36:3, 36:7, 36:8, 36:18, 38:16, 45:23, 46:18, 54:12, 59:9, 63:18, 63:24, 66:18, 66:21, 72:21, 78:13, 79:4, 91:11, 91:21, 92:10, 102:21 running [20] - 34:5, 34:10, 36:9, 36:11, 37:15, 37:24, 39:7, 40:7, 40:9, 40:11, 44:12, 49:13, 54:23, 57:4, 58:24, 91:13, 91:14, 91:15, 91:16, 92:5 runs [5] - 22:25, 24:14, 28:24, 34:23</p>	<p>scenarios [1] - 114:5 school [2] - 21:12, 21:14 science [5] - 20:12, 21:4, 21:6, 21:8, 21:25 scope [2] - 72:15, 74:2 screen [4] - 4:6, 58:18, 58:19 search [11] - 8:14, 8:19, 10:3, 14:10, 22:18, 22:19, 26:7, 74:2, 79:9, 117:25, 118:6 second [8] - 20:14, 30:6, 44:11, 83:23, 107:1, 108:20, 110:2, 110:12 secondary [1] - 11:9 secondly [2] - 9:16, 13:19 seconds [5] - 7:19, 53:22, 54:2, 73:22, 76:25 section [1] - 70:14 Section [1] - 124:6 security [9] - 20:12, 39:17, 86:5, 87:3, 87:11, 90:5, 91:12, 93:19, 108:4 see [24] - 23:6, 43:22, 44:4, 53:3, 57:10, 58:25, 62:19, 65:1, 67:20, 72:22, 72:25, 73:8, 73:12, 73:14, 74:17, 91:17, 91:24, 92:14, 92:18, 93:2, 94:17, 108:2 seeing [3] - 41:15, 67:15, 112:23 seek [2] - 11:23, 120:13 seeking [4] - 14:14, 14:15, 15:24, 109:10 seeks [1] - 11:7 seem [2] - 112:7, 112:17 seize [2] - 79:13, 79:15 seized [3] - 10:2, 91:3, 91:5 send [9] - 7:3, 16:17, 28:4, 28:5, 28:23, 28:25, 72:23, 73:15, 73:17 sending [4] - 7:17, 7:25, 54:24, 58:13 sends [2] - 54:13, 75:18 sense [8] - 14:2,</p>	<p>57:17, 57:20, 58:6, 89:11, 102:25, 107:15, 114:23 sensitive [10] - 11:15, 48:14, 82:9, 82:18, 82:22, 82:23, 97:3, 97:4, 97:6, 120:22 sent [23] - 6:16, 6:25, 7:12, 7:23, 8:2, 9:10, 9:14, 13:25, 16:2, 16:5, 16:20, 22:19, 27:2, 28:20, 29:7, 30:7, 31:8, 31:16, 63:18, 73:13, 73:19, 76:14, 95:7 separate [13] - 13:4, 14:5, 19:10, 77:4, 77:8, 85:16, 85:17, 88:7, 93:24, 96:17, 97:19, 97:21, 98:8 series [1] - 17:6 serve [1] - 80:7 server [44] - 18:21, 24:24, 27:15, 27:18, 27:19, 28:1, 29:1, 29:4, 29:8, 29:10, 29:12, 30:9, 30:10, 38:22, 39:1, 39:2, 39:7, 39:10, 39:21, 40:8, 40:9, 40:10, 40:19, 48:23, 49:10, 53:21, 69:1, 72:25, 73:10, 73:14, 73:15, 74:11, 74:12, 74:13, 75:4, 84:8, 90:10, 94:5, 94:14, 94:16, 102:17, 103:20, 107:4, 107:12 servers [2] - 24:16, 85:20 serves [1] - 79:14 service [1] - 8:7 services [3] - 84:5, 92:10, 93:17 session [2] - 77:3 sessions [2] - 76:12, 76:23 set [7] - 18:9, 44:13, 52:15, 56:23, 57:5, 116:24, 122:16 setting [2] - 46:9, 46:23 settings [10] - 35:10, 36:7, 36:14, 36:15, 53:13, 91:9, 91:12, 92:2, 92:6, 108:4 several [6] - 9:5, 22:2, 45:6, 96:1, 115:10, 117:21 sexual [2] - 3:12, 3:14</p>	<p>share [2] - 119:11, 122:3 shelf [1] - 82:20 shift [1] - 17:12 short [1] - 6:12 Short [1] - 62:23 shorthand [1] - 1:21 show [2] - 101:24, 106:13 showed [1] - 31:16 shown [1] - 114:5 side [4] - 7:25, 36:22, 36:23, 91:23 sides [1] - 17:10 sign [2] - 96:13, 122:11 sign-on [1] - 96:13 significance [1] - 74:7 significant [3] - 85:18, 87:4, 112:8 signs [1] - 91:19 similar [5] - 5:13, 26:2, 39:3, 66:23, 91:15 simply [2] - 10:24, 110:18 sincere [1] - 115:4 single [4] - 41:18, 93:19, 93:20, 117:10 site [1] - 89:14 sites [1] - 58:4 sitting [1] - 115:12 situation [2] - 53:19, 58:17 situations [3] - 38:16, 48:8, 48:19 six [2] - 7:3, 8:25 skeptically [1] - 102:25 slack [1] - 61:7 slightly [1] - 85:10 small [1] - 71:6 smart [1] - 32:21 Smith [1] - 1:14 so-called [2] - 13:6, 15:25 so.. [1] - 62:20 Social [1] - 35:22 Social-Engineer [1] - 35:22 software [51] - 10:10, 10:23, 10:25, 12:11, 16:12, 16:14, 18:20, 21:18, 23:2, 24:1, 26:17, 26:22, 28:13, 28:14, 29:17, 32:1, 32:3, 33:4, 33:10, 33:19, 34:10, 34:20, 37:17, 37:19, 37:22, 38:7, 40:7, 41:7,</p>	<p>41:9, 43:18, 52:3, 58:23, 59:4, 59:5, 59:10, 59:22, 59:23, 65:18, 80:2, 80:7, 80:24, 81:8, 83:24, 91:22, 91:24, 92:19, 92:25, 93:5, 102:16 softwares [1] - 33:3 Soghoian [1] - 47:19 someone [18] - 53:24, 67:11, 67:18, 68:3, 83:10, 83:17, 84:9, 85:3, 86:1, 86:5, 86:11, 86:23, 89:2, 104:4, 106:15, 108:15, 119:7 somewhat [2] - 6:4, 119:25 somewhere [3] - 28:2, 60:2, 71:14 soon [1] - 118:18 sophisticated [8] - 55:19, 56:5, 56:23, 57:21, 58:14, 87:15, 87:16, 87:17 sophistication [2] - 83:7, 89:16 sorry [7] - 25:24, 27:19, 54:18, 62:24, 90:9, 95:5, 111:9 sort [14] - 16:1, 32:18, 35:6, 39:17, 55:7, 61:5, 61:6, 61:9, 82:14, 82:15, 109:2, 120:24, 122:16, 122:17 sorts [1] - 59:7 sound [3] - 47:25, 67:14, 113:15 sounds [5] - 17:25, 50:12, 90:23, 91:6, 101:6 source [37] - 12:4, 13:9, 22:12, 22:15, 22:16, 22:23, 22:24, 23:1, 23:7, 23:11, 23:19, 24:18, 31:4, 31:7, 34:1, 34:16, 63:16, 63:19, 64:18, 64:23, 64:25, 65:1, 65:6, 65:20, 66:6, 66:12, 67:15, 67:21, 68:7, 68:10, 68:13, 68:15, 78:19, 97:24, 98:4, 109:13, 110:3 space [1] - 61:7 span [2] - 7:18, 112:8 speaking [1] - 16:21 Special [3] - 69:24, 113:24, 117:12</p>
S				
<p>safe [2] - 21:22, 41:23 sake [1] - 80:12 save [2] - 28:2, 94:7 saved [3] - 40:4, 94:3, 94:9 saving [1] - 40:2 scale [2] - 60:10, 103:7 scenario [1] - 41:18</p>	<p>seconds [5] - 7:19, 53:22, 54:2, 73:22, 76:25 section [1] - 70:14 Section [1] - 124:6 security [9] - 20:12, 39:17, 86:5, 87:3, 87:11, 90:5, 91:12, 93:19, 108:4 see [24] - 23:6, 43:22, 44:4, 53:3, 57:10, 58:25, 62:19, 65:1, 67:20, 72:22, 72:25, 73:8, 73:12, 73:14, 74:17, 91:17, 91:24, 92:14, 92:18, 93:2, 94:17, 108:2 seeing [3] - 41:15, 67:15, 112:23 seek [2] - 11:23, 120:13 seeking [4] - 14:14, 14:15, 15:24, 109:10 seeks [1] - 11:7 seem [2] - 112:7, 112:17 seize [2] - 79:13, 79:15 seized [3] - 10:2, 91:3, 91:5 send [9] - 7:3, 16:17, 28:4, 28:5, 28:23, 28:25, 72:23, 73:15, 73:17 sending [4] - 7:17, 7:25, 54:24, 58:13 sends [2] - 54:13, 75:18 sense [8] - 14:2,</p>	<p>57:17, 57:20, 58:6, 89:11, 102:25, 107:15, 114:23 sensitive [10] - 11:15, 48:14, 82:9, 82:18, 82:22, 82:23, 97:3, 97:4, 97:6, 120:22 sent [23] - 6:16, 6:25, 7:12, 7:23, 8:2, 9:10, 9:14, 13:25, 16:2, 16:5, 16:20, 22:19, 27:2, 28:20, 29:7, 30:7, 31:8, 31:16, 63:18, 73:13, 73:19, 76:14, 95:7 separate [13] - 13:4, 14:5, 19:10, 77:4, 77:8, 85:16, 85:17, 88:7, 93:24, 96:17, 97:19, 97:21, 98:8 series [1] - 17:6 serve [1] - 80:7 server [44] - 18:21, 24:24, 27:15, 27:18, 27:19, 28:1, 29:1, 29:4, 29:8, 29:10, 29:12, 30:9, 30:10, 38:22, 39:1, 39:2, 39:7, 39:10, 39:21, 40:8, 40:9, 40:10, 40:19, 48:23, 49:10, 53:21, 69:1, 72:25, 73:10, 73:14, 73:15, 74:11, 74:12, 74:13, 75:4, 84:8, 90:10, 94:5, 94:14, 94:16, 102:17, 103:20, 107:4, 107:12 servers [2] - 24:16, 85:20 serves [1] - 79:14 service [1] - 8:7 services [3] - 84:5, 92:10, 93:17 session [2] - 77:3 sessions [2] - 76:12, 76:23 set [7] - 18:9, 44:13, 52:15, 56:23, 57:5, 116:24, 122:16 setting [2] - 46:9, 46:23 settings [10] - 35:10, 36:7, 36:14, 36:15, 53:13, 91:9, 91:12, 92:2, 92:6, 108:4 several [6] - 9:5, 22:2, 45:6, 96:1, 115:10, 117:21 sexual [2] - 3:12, 3:14</p>	<p>share [2] - 119:11, 122:3 shelf [1] - 82:20 shift [1] - 17:12 short [1] - 6:12 Short [1] - 62:23 shorthand [1] - 1:21 show [2] - 101:24, 106:13 showed [1] - 31:16 shown [1] - 114:5 side [4] - 7:25, 36:22, 36:23, 91:23 sides [1] - 17:10 sign [2] - 96:13, 122:11 sign-on [1] - 96:13 significance [1] - 74:7 significant [3] - 85:18, 87:4, 112:8 signs [1] - 91:19 similar [5] - 5:13, 26:2, 39:3, 66:23, 91:15 simply [2] - 10:24, 110:18 sincere [1] - 115:4 single [4] - 41:18, 93:19, 93:20, 117:10 site [1] - 89:14 sites [1] - 58:4 sitting [1] - 115:12 situation [2] - 53:19, 58:17 situations [3] - 38:16, 48:8, 48:19 six [2] - 7:3, 8:25 skeptically [1] - 102:25 slack [1] - 61:7 slightly [1] - 85:10 small [1] - 71:6 smart [1] - 32:21 Smith [1] - 1:14 so-called [2] - 13:6, 15:25 so.. [1] - 62:20 Social [1] - 35:22 Social-Engineer [1] - 35:22 software [51] - 10:10, 10:23, 10:25, 12:11, 16:12, 16:14, 18:20, 21:18, 23:2, 24:1, 26:17, 26:22, 28:13, 28:14, 29:17, 32:1, 32:3, 33:4, 33:10, 33:19, 34:10, 34:20, 37:17, 37:19, 37:22, 38:7, 40:7, 41:7,</p>	<p>41:9, 43:18, 52:3, 58:23, 59:4, 59:5, 59:10, 59:22, 59:23, 65:18, 80:2, 80:7, 80:24, 81:8, 83:24, 91:22, 91:24, 92:19, 92:25, 93:5, 102:16 softwares [1] - 33:3 Soghoian [1] - 47:19 someone [18] - 53:24, 67:11, 67:18, 68:3, 83:10, 83:17, 84:9, 85:3, 86:1, 86:5, 86:11, 86:23, 89:2, 104:4, 106:15, 108:15, 119:7 somewhat [2] - 6:4, 119:25 somewhere [3] - 28:2, 60:2, 71:14 soon [1] - 118:18 sophisticated [8] - 55:19, 56:5, 56:23, 57:21, 58:14, 87:15, 87:16, 87:17 sophistication [2] - 83:7, 89:16 sorry [7] - 25:24, 27:19, 54:18, 62:24, 90:9, 95:5, 111:9 sort [14] - 16:1, 32:18, 35:6, 39:17, 55:7, 61:5, 61:6, 61:9, 82:14, 82:15, 109:2, 120:24, 122:16, 122:17 sorts [1] - 59:7 sound [3] - 47:25, 67:14, 113:15 sounds [5] - 17:25, 50:12, 90:23, 91:6, 101:6 source [37] - 12:4, 13:9, 22:12, 22:15, 22:16, 22:23, 22:24, 23:1, 23:7, 23:11, 23:19, 24:18, 31:4, 31:7, 34:1, 34:16, 63:16, 63:19, 64:18, 64:23, 64:25, 65:1, 65:6, 65:20, 66:6, 66:12, 67:15, 67:21, 68:7, 68:10, 68:13, 68:15, 78:19, 97:24, 98:4, 109:13, 110:3 space [1] - 61:7 span [2] - 7:18, 112:8 speaking [1] - 16:21 Special [3] - 69:24, 113:24, 117:12</p>

<p>special [2] - 70:11, 70:18</p> <p>specialized [1] - 22:5</p> <p>specific [11] - 7:7, 7:9, 9:13, 23:22, 28:9, 53:19, 60:20, 64:24, 83:15, 92:9, 107:17</p> <p>specifically [7] - 4:14, 9:9, 12:21, 15:19, 41:20, 44:24, 109:22</p> <p>specifics [1] - 61:4</p> <p>speculation [3] - 113:24, 114:19, 116:8</p> <p>spelled [1] - 70:11</p> <p>squeeze [1] - 89:17</p> <p>stable [1] - 119:6</p> <p>stage [1] - 106:5</p> <p>stand [1] - 19:16</p> <p>standard [4] - 48:11, 104:22, 114:16, 114:18</p> <p>standby [1] - 69:15</p> <p>stands [1] - 71:13</p> <p>start [4] - 17:12, 22:23, 29:15, 65:22</p> <p>starting [2] - 15:25, 60:3</p> <p>starting-out [1] - 15:25</p> <p>stat [1] - 88:6</p> <p>State [3] - 21:1, 22:4, 24:7</p> <p>state [6] - 4:21, 18:5, 20:5, 44:25, 93:15, 103:8</p> <p>statement [9] - 12:2, 45:4, 46:13, 47:8, 48:1, 77:6, 88:25, 111:17, 113:22</p> <p>statements [1] - 75:9</p> <p>STATES [2] - 1:1, 1:3</p> <p>States [7] - 1:13, 3:2, 3:4, 72:3, 124:4, 124:6, 124:11</p> <p>statically [1] - 37:5</p> <p>stating [2] - 3:21, 61:14</p> <p>Steele [1] - 1:18</p> <p>stenographically [1] - 124:8</p> <p>step [9] - 28:18, 29:19, 29:20, 30:8, 30:12, 32:1, 38:24, 80:11, 99:14</p> <p>steps [1] - 17:7</p> <p>still [9] - 17:16, 80:13, 80:21, 80:24, 82:22, 88:8, 114:22, 115:1, 121:17</p>	<p>still-sensitive [1] - 82:22</p> <p>stock [2] - 113:10, 113:14</p> <p>stop [2] - 42:16, 42:22</p> <p>storage [7] - 48:23, 49:4, 49:17, 74:13, 74:21, 74:23, 75:4</p> <p>stored [17] - 15:1, 18:22, 19:4, 19:9, 40:1, 41:2, 49:11, 75:1, 76:7, 94:10, 94:13, 94:18, 94:20, 94:21, 103:20, 103:22, 107:13</p> <p>storing [2] - 49:10, 94:22</p> <p>straightforward [1] - 113:21</p> <p>strategy [1] - 102:13</p> <p>stream [15] - 9:17, 19:6, 19:10, 29:6, 31:15, 41:5, 44:16, 44:17, 47:5, 47:20, 66:24, 73:1, 73:4, 73:7, 74:8</p> <p>streams [2] - 25:1, 55:17</p> <p>Street [2] - 1:24, 37:1</p> <p>strictly [1] - 120:25</p> <p>string [1] - 6:15</p> <p>stronger [1] - 82:16</p> <p>structure [1] - 92:8</p> <p>stuff [3] - 17:13, 67:25, 87:6</p> <p>subject [3] - 66:19, 109:4, 113:11</p> <p>submitted [4] - 8:6, 25:18, 25:21, 102:3</p> <p>subpoena [3] - 8:7, 8:11, 116:15</p> <p>subpoenas [1] - 50:9</p> <p>subscriber [1] - 8:12</p> <p>subsequent [1] - 96:14</p> <p>substance [1] - 42:22</p> <p>substantial [1] - 59:2</p> <p>subtract [1] - 14:12</p> <p>successfully [1] - 96:11</p> <p>sufficient [4] - 37:16, 41:1, 51:22, 122:20</p> <p>sufficiently [1] - 103:2</p> <p>suggest [1] - 85:12</p> <p>Suite [1] - 1:18</p> <p>summarize [1] - 21:10</p> <p>summer [1] - 42:20</p> <p>super [1] - 8:16</p> <p>superfluous [1] - 105:14</p>	<p>superseding [2] - 3:10, 117:6</p> <p>supplement [1] - 5:6</p> <p>supply [1] - 41:9</p> <p>suppose [1] - 33:16</p> <p>supposed [5] - 26:20, 28:5, 61:25, 114:12, 116:20</p> <p>suppress [2] - 3:22, 70:24</p> <p>suppression [11] - 5:17, 7:5, 7:16, 7:21, 10:20, 71:17, 88:15, 103:8, 117:3, 118:21, 120:8</p> <p>surreptitiously [1] - 60:11</p> <p>sustain [1] - 89:21</p> <p>sworn [3] - 19:24, 20:2, 70:4</p> <p>synonym [1] - 81:7</p> <p>synonymous [3] - 18:6, 46:12, 63:3</p> <p>synonymously [1] - 16:11</p> <p>system [22] - 7:10, 21:19, 26:24, 27:1, 34:3, 34:11, 34:20, 35:24, 39:14, 39:17, 41:3, 41:6, 43:19, 45:1, 45:25, 46:18, 46:20, 51:20, 90:5, 91:15, 91:17, 92:3</p> <p>systems [5] - 21:17, 31:18, 34:3, 37:12, 59:21</p>	<p>82:19</p> <p>technology [4] - 82:21, 82:22, 100:20, 100:22</p> <p>teleconference [1] - 4:5</p> <p>temporarily [1] - 46:1</p> <p>temporary [2] - 26:25, 45:20</p> <p>ten [2] - 32:10, 61:25</p> <p>tend [1] - 37:23</p> <p>tends [1] - 119:24</p> <p>term [12] - 12:25, 16:10, 18:1, 22:7, 29:9, 63:2, 63:3, 63:4, 63:19, 63:20, 63:21</p> <p>terminology [7] - 4:3, 5:18, 5:25, 10:18, 12:14, 15:4, 18:14</p> <p>terms [4] - 4:23, 6:8, 48:24, 53:25</p> <p>terrible [1] - 37:3</p> <p>test [13] - 13:17, 36:11, 37:12, 37:17, 38:14, 38:20, 38:21, 66:22, 91:12, 91:18, 100:3, 105:22, 105:25</p> <p>tested [7] - 72:19, 74:2, 79:20, 91:16, 100:24</p> <p>testified [24] - 5:13, 20:2, 38:23, 47:5, 47:19, 47:22, 52:3, 53:18, 62:6, 70:4, 70:22, 77:21, 79:21, 81:15, 81:20, 84:3, 94:2, 103:2, 109:11, 109:15, 109:19, 113:25, 119:1, 122:1</p> <p>testify [4] - 15:15, 19:8, 19:11, 77:16</p> <p>testifying [6] - 4:16, 5:11, 47:9, 62:12, 71:22, 71:24</p> <p>testimony [35] - 5:16, 7:16, 7:20, 12:8, 12:9, 15:19, 47:23, 53:15, 59:25, 71:1, 71:7, 71:19, 71:21, 75:9, 76:2, 79:1, 79:5, 83:1, 83:8, 88:24, 95:7, 97:14, 101:4, 102:2, 102:4, 102:24, 106:21, 106:25, 109:20, 113:15, 113:16, 115:3, 115:4, 117:12, 120:21</p>	<p>testing [3] - 23:23, 24:5, 37:17</p> <p>text [2] - 7:13, 13:20</p> <p>THE [94] - 1:9, 1:11, 1:16, 3:1, 3:7, 3:8, 4:10, 4:19, 12:12, 12:16, 12:24, 15:8, 15:20, 16:24, 17:8, 18:8, 18:11, 18:25, 19:5, 19:12, 19:17, 19:19, 19:20, 42:3, 42:5, 51:4, 51:7, 52:11, 52:13, 62:24, 62:25, 67:1, 67:24, 69:10, 69:13, 69:19, 69:22, 70:1, 70:5, 86:17, 88:18, 89:4, 89:10, 90:15, 90:18, 95:17, 95:21, 99:7, 99:11, 99:13, 99:15, 99:16, 99:19, 99:21, 100:1, 104:20, 106:2, 106:20, 107:16, 108:7, 108:10, 108:19, 109:8, 109:25, 110:8, 110:13, 110:15, 110:23, 111:4, 111:7, 111:11, 111:20, 111:23, 111:25, 112:25, 113:3, 113:6, 114:21, 117:5, 117:15, 117:17, 118:4, 118:11, 118:13, 118:16, 119:10, 119:22, 120:15, 121:11, 121:19, 121:22, 122:8, 122:24, 123:1</p> <p>themselves [1] - 54:5</p> <p>theoretical [4] - 53:12, 56:2, 62:14, 85:11</p> <p>theories [1] - 106:12</p> <p>theory [6] - 60:18, 105:8, 105:12, 105:17, 106:5, 118:24</p> <p>therefore [1] - 89:14</p> <p>they've [1] - 15:13</p> <p>third [11] - 9:21, 17:16, 30:8, 35:14, 53:14, 54:20, 59:9, 60:10, 77:12, 108:5, 109:5</p> <p>third-party [3] - 35:14, 108:5, 109:5</p> <p>thousand [1] - 103:10</p> <p>thousands [4] - 71:11, 71:12, 71:15, 103:12</p>
T				
<p>Tacoma [1] - 25:13</p> <p>tampered [1] - 75:2</p> <p>target [1] - 58:5</p> <p>TCP [7] - 47:6, 47:14, 48:2, 48:4, 48:11, 48:20</p> <p>teach [2] - 20:11, 20:12</p> <p>team [6] - 101:8, 119:12, 119:18, 120:6, 120:7</p> <p>teamers [4] - 56:11, 56:16, 83:5</p> <p>teams [1] - 59:7</p> <p>technical [1] - 87:4</p> <p>technically [1] - 57:25</p> <p>technique [2] - 6:13, 56:19</p> <p>techniques [3] - 11:16, 56:9, 85:17</p> <p>technologies [1] -</p>				

<p>three [4] - 17:3, 45:11, 45:12, 120:18</p> <p>throughout [1] - 120:16</p> <p>thrown [1] - 103:9</p> <p>tie [1] - 41:4</p> <p>tied [1] - 93:10</p> <p>timeframe [1] - 90:25</p> <p>TIMOTHY [1] - 1:9</p> <p>tiny [1] - 85:9</p> <p>Title [1] - 124:6</p> <p>today [10] - 3:8, 20:16, 75:10, 76:2, 77:16, 113:15, 113:19, 115:10, 120:17, 122:22</p> <p>together [2] - 28:23, 122:9</p> <p>took [7] - 46:19, 46:22, 46:24, 61:1, 73:21, 106:15, 117:7</p> <p>toolkit [1] - 35:22</p> <p>tools [12] - 11:16, 35:21, 50:5, 50:21, 73:25, 74:5, 75:17, 80:14, 82:18, 85:5, 85:17, 104:1</p> <p>top [1] - 92:8</p> <p>Tor [32] - 7:24, 10:10, 10:15, 13:6, 25:3, 53:20, 55:4, 55:6, 56:25, 57:4, 57:9, 58:10, 67:14, 68:3, 71:10, 71:13, 82:13, 83:15, 84:1, 84:2, 84:4, 84:5, 84:19, 84:22, 85:6, 85:16, 85:22, 85:24, 85:25, 86:6, 87:18, 108:21</p> <p>total [1] - 17:5</p> <p>touched [1] - 74:11</p> <p>trace [2] - 50:9, 112:16</p> <p>track [2] - 76:6, 76:21</p> <p>tracked [1] - 14:7</p> <p>tracking [2] - 38:7, 76:11</p> <p>traffic [3] - 83:25, 84:1, 84:18</p> <p>training [12] - 22:6, 22:9, 22:10, 23:22, 26:16, 31:24, 33:24, 38:6, 38:24, 40:24, 56:18, 87:20</p> <p>trainings [1] - 24:6</p> <p>transaction [1] - 21:21</p> <p>transcript [5] - 71:3, 71:5, 71:9, 124:7, 124:9</p> <p>TRANSCRIPT [1] - 1:8</p> <p>transfer [1] - 47:16</p>	<p>transferring [1] - 47:15</p> <p>translates [1] - 65:19</p> <p>translation [1] - 23:9</p> <p>transmission [3] - 14:3, 48:12, 48:14</p> <p>transmitted [1] - 7:6</p> <p>travel [1] - 36:24</p> <p>trial [3] - 100:25, 102:13, 104:16</p> <p>trigger [1] - 96:16</p> <p>true [5] - 8:4, 49:7, 104:3, 106:2, 124:7</p> <p>trust [1] - 34:8</p> <p>try [3] - 35:2, 115:18, 120:24</p> <p>trying [13] - 6:7, 23:16, 45:18, 56:10, 56:12, 57:20, 59:14, 59:19, 59:20, 89:17, 98:1, 107:3, 115:19</p> <p>Tsyrklevich [4] - 25:19, 111:6, 111:8, 111:9</p> <p>Tsyrklevich's [1] - 110:19</p> <p>turn [2] - 24:12, 90:19</p> <p>turned [20] - 9:25, 10:4, 13:4, 15:11, 15:13, 15:16, 15:17, 24:13, 73:4, 75:6, 75:8, 75:20, 75:22, 77:11, 77:17, 81:10, 81:20, 81:25, 82:5</p> <p>turning [1] - 78:21</p> <p>turns [1] - 114:22</p> <p>TV [1] - 4:6</p> <p>two [27] - 9:17, 17:10, 19:5, 19:10, 25:1, 29:6, 31:15, 44:16, 44:17, 56:17, 65:11, 73:4, 73:7, 73:23, 74:8, 74:19, 75:5, 77:10, 85:18, 95:10, 97:19, 109:17, 109:25, 110:1, 110:5, 112:16, 120:18</p> <p>two-way [12] - 9:17, 19:5, 19:10, 25:1, 29:6, 31:15, 44:16, 44:17, 73:4, 73:7, 74:8, 95:10</p> <p>Tyler [1] - 62:22</p> <p>type [16] - 25:11, 33:13, 34:25, 43:17, 58:4, 58:21, 59:4, 59:5, 59:22, 67:8, 81:8, 87:6, 93:5, 101:23, 105:22,</p>	<p>122:19</p> <p>types [2] - 43:25, 87:5</p> <p>typically [3] - 39:13, 43:17, 77:21</p>	<p style="text-align: center;">U</p> <p>U.S [1] - 42:9</p> <p>Ubuntu [1] - 92:4</p> <p>ultimately [2] - 50:6, 120:3</p> <p>umbrella [1] - 17:4</p> <p>unanticipated [1] - 36:17</p> <p>unauthorized [1] - 39:11</p> <p>uncertain [1] - 8:24</p> <p>under [9] - 2:19, 6:19, 11:3, 98:19, 98:23, 109:15, 114:1, 118:17, 119:5</p> <p>unencrypted [1] - 7:14</p> <p>unexpected [2] - 33:7, 35:1</p> <p>unin [1] - 34:9</p> <p>unintended [10] - 33:11, 34:5, 34:10, 91:22, 93:17, 93:22, 93:25, 103:14, 115:9, 120:2</p> <p>unintentional [1] - 93:4</p> <p>unintentionally [1] - 75:3</p> <p>unique [80] - 7:6, 14:19, 14:20, 14:23, 15:5, 15:25, 16:15, 17:23, 18:20, 24:19, 27:13, 27:15, 28:2, 28:10, 28:12, 29:5, 29:17, 29:24, 32:2, 32:3, 33:19, 61:13, 61:18, 62:8, 69:4, 69:7, 75:24, 76:1, 76:3, 76:5, 76:10, 76:13, 76:16, 76:17, 76:21, 76:24, 77:2, 77:4, 77:7, 78:21, 80:3, 80:5, 80:10, 80:13, 80:20, 80:21, 80:22, 89:24, 90:9, 94:2, 94:8, 94:10, 94:13, 94:18, 96:21, 96:23, 97:2, 97:5, 100:18, 100:19, 102:17, 103:3, 103:5, 103:6, 103:11, 103:15, 107:5, 108:17, 108:19, 109:9,</p>	<p>110:4, 118:25, 120:20, 121:14, 122:3</p> <p>unit [1] - 70:14</p> <p>UNITED [2] - 1:1, 1:3</p> <p>United [7] - 1:13, 3:2, 3:4, 72:3, 124:4, 124:6, 124:11</p> <p>universe [4] - 5:19, 5:20, 14:11, 31:23</p> <p>University [6] - 20:9, 20:14, 20:24, 21:1, 22:4, 24:7</p> <p>university [1] - 24:3</p> <p>unless [4] - 10:24, 12:22, 15:22, 19:13</p> <p>unlikely [7] - 58:1, 58:3, 60:2, 60:5, 112:9, 116:2, 116:7</p> <p>unreliable [1] - 47:21</p> <p>up [27] - 4:20, 16:4, 16:6, 23:5, 34:25, 37:2, 41:17, 44:13, 51:17, 52:15, 55:8, 56:23, 57:5, 57:23, 62:8, 62:9, 64:8, 65:15, 66:5, 66:9, 68:22, 76:17, 78:3, 92:11, 92:15, 112:19, 116:22</p> <p>update [1] - 51:19</p> <p>updated [3] - 32:17, 32:19, 32:22</p> <p>useful [5] - 39:24, 43:24, 105:4, 109:11, 122:2</p> <p>usefulness [1] - 107:20</p> <p>useless [1] - 102:12</p> <p>user [25] - 6:20, 9:23, 27:24, 28:9, 34:7, 38:18, 41:4, 41:11, 48:7, 48:19, 55:19, 58:11, 58:17, 76:6, 76:11, 76:15, 76:22, 78:4, 78:8, 83:15, 87:10, 96:12, 96:13, 107:7</p> <p>user's [8] - 28:20, 30:8, 49:25, 52:21, 94:5, 94:7, 94:9</p> <p>user-friendly [2] - 78:4, 78:8</p> <p>username [4] - 14:21, 14:24, 50:7, 107:5</p> <p>usernames [1] - 33:21</p> <p>users [9] - 25:3, 27:14, 27:22, 38:11, 39:12, 54:24, 87:14, 87:22, 103:10</p>	<p>users' [1] - 6:16</p> <p>uses [1] - 85:19</p> <p>utilized [2] - 10:10, 10:12</p> <p>utilizing [1] - 86:12</p>	<p style="text-align: center;">V</p> <p>vacation [1] - 42:21</p> <p>value [2] - 8:25, 43:21</p> <p>variant [1] - 92:4</p> <p>variety [1] - 37:12</p> <p>various [4] - 76:22, 87:21, 92:12, 92:13</p> <p>vary [1] - 34:4</p> <p>verbatim [1] - 104:21</p> <p>verified [3] - 22:18, 34:17, 100:24</p> <p>verify [18] - 22:17, 25:15, 37:6, 37:11, 37:20, 38:15, 39:4, 39:11, 44:16, 49:15, 50:4, 64:15, 69:3, 72:14, 73:24, 73:25, 98:21, 102:25</p> <p>verifying [1] - 39:19</p> <p>version [9] - 28:7, 28:8, 63:10, 63:13, 63:15, 97:1, 98:2, 109:16</p> <p>versions [1] - 109:17</p> <p>versus [5] - 3:2, 23:15, 72:3, 87:18, 112:22</p> <p>via [9] - 1:21, 2:8, 4:5, 7:23, 30:11, 69:15, 69:17, 69:18</p> <p>viable [1] - 82:11</p> <p>video [3] - 69:15, 69:17</p> <p>videoconference [1] - 2:8</p> <p>view [3] - 3:15, 58:20</p> <p>viewed [2] - 33:15, 59:1</p> <p>viewing [3] - 58:18, 58:22, 58:23</p> <p>violate [1] - 43:14</p> <p>violations [1] - 120:1</p> <p>Violent [1] - 70:13</p> <p>Virginia [1] - 26:1</p> <p>virtual [1] - 91:14</p> <p>visit [2] - 42:16, 96:14</p> <p>visited [2] - 32:6, 41:13</p> <p>visiting [1] - 58:4</p> <p>visual [1] - 98:14</p> <p>VS [1] - 1:5</p> <p>vulnerable [6] - 35:13, 93:6, 93:7, 93:15, 104:6, 108:4</p>
---	---	---	--	--	--	--

W	WITNESSES [2] - 2:7, 2:12
<p>wait [1] - 106:20 waiting [1] - 56:6 walk [1] - 36:22 wants [2] - 12:19, 115:14 warrant [14] - 8:14, 8:19, 10:3, 14:10, 22:18, 22:19, 26:7, 72:16, 72:23, 73:2, 74:2, 79:9, 117:25, 118:6 Washington [2] - 25:13, 44:22 ways [3] - 28:21, 36:23, 40:11 web [1] - 14:7 website [50] - 6:19, 10:11, 14:8, 19:2, 27:21, 32:6, 39:4, 43:8, 50:7, 54:25, 55:12, 56:24, 57:10, 58:19, 60:9, 60:21, 61:2, 61:16, 76:6, 76:12, 76:22, 77:6, 80:16, 83:13, 83:16, 83:19, 84:6, 84:10, 84:12, 84:17, 85:25, 86:6, 86:9, 86:10, 86:14, 86:22, 87:2, 87:10, 87:13, 87:22, 95:23, 95:24, 96:1, 96:18, 98:18, 98:19, 98:23, 103:10, 114:2 websites [4] - 34:8, 67:8, 84:21, 85:19 weighed [1] - 101:3 weird [1] - 49:21 well-known [1] - 82:10 Western [1] - 124:5 WESTERN [1] - 1:1 what-ifs [2] - 114:6, 115:2 whole [8] - 17:8, 50:10, 83:8, 113:9, 113:13, 114:7, 114:15, 115:13 wholly [1] - 105:14 wild [1] - 87:24 willing [2] - 105:16, 120:16 windows [1] - 32:21 Windows [1] - 33:1 withholding [1] - 98:7 WITNESS [3] - 19:19, 62:25, 99:15 witness [8] - 4:2, 4:4, 19:24, 35:25, 42:2, 69:18, 101:3, 109:11</p>	<p>witnesses [6] - 69:20, 69:21, 99:17, 107:21, 107:22, 113:10 word [4] - 13:15, 57:18, 81:14, 100:17 worded [1] - 49:21 words [1] - 10:23 works [2] - 45:25, 55:16 world [4] - 46:25, 50:13, 71:14, 80:16 worth [1] - 73:3 wrap [1] - 45:18 write [20] - 23:25, 24:21, 28:13, 28:14, 28:16, 31:6, 35:2, 35:19, 38:13, 63:22, 63:24, 89:23, 90:1, 90:9, 90:10, 102:19, 104:21, 112:15 writing [2] - 64:15, 121:23 written [11] - 28:11, 33:7, 33:10, 39:9, 68:14, 71:20, 77:22, 78:7, 78:10, 78:13, 98:4</p>
	Y
	<p>y'all [2] - 45:11, 122:9 year [1] - 20:14 years [1] - 21:15 yield [2] - 102:8, 102:9 Yon [1] - 25:19 yourself [4] - 25:19, 38:9, 55:21, 70:9</p>
	Z
	<p>zero [3] - 85:9, 85:10, 86:14</p>