

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

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

- - - - -		
UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	CRIMINAL CASE NO.
v.)	4:16cr00016
)	
EDWARD JOSEPH MATISH, III,)	
)	
Defendant.)	
- - - - -		

EXCERPT OF PROCEEDINGS
(Testimony of Special Agent Daniel Alfin)

Norfolk, Virginia
May 19, 2016

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

UNITED STATES ATTORNEY'S OFFICE
By: Eric M. Hurt
Kaitlin C. Gratton
Assistant United States Attorneys
Counsel for the United States

FEDERAL PUBLIC DEFENDER'S OFFICE
By: Andrew W. Grindrod
Richard J. Colgan
Assistant Federal Public Defenders
Counsel for the Defendant

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

I N D E X

ON BEHALF OF THE DEFENDANT:	Direct	Cross	Red.	Rec.
D. Alfin	3	32	48	--

E X H I B I T S

No.		Page
Defendant's Exhibit 5 (sealed)		30
Defendant's Exhibit 2		30
Defendant's Exhibit 3		30
Defendant's Exhibit 4		36

—D. Alfin - Direct—

1 assigned to FBI Headquarters, Criminal Investigative
2 Division, Violent Crimes Against Children Section, Major Case
3 Coordination Unit.

4 Q. Thank you, sir. You were involved in the investigation
5 of the Playpen Web site from pretty early on, right?

6 A. I was involved in this investigation, yes.

7 Q. Okay. Just by way of background, at some point the FBI
8 came across this Playpen site, correct?

9 A. The Playpen Web site came online approximately August,
10 2014. It came to my attention at that time.

11 Q. And you eventually determined around that same time that
12 there was child pornography present on the Web site?

13 A. Immediately after Playpen came online and after viewing
14 it I observed that it was a Web site whose primary purpose
15 was the advertisement and distribution of child pornography.

16 Q. And, so, you began investigating to try to find out who
17 the administrator of the Web site was, correct?

18 A. We eventually received information that we followed up on
19 and led us to the identification of the administrator of the
20 Web site.

21 Q. And, generally, what time period was that?

22 A. We received information about the Playpen Web site in
23 approximately December, 2014.

24 Q. And between August of 2014, when you say the site came
25 online, and December of 2014 you and the FBI were

—D. Alfin - Direct—

1 continuously monitoring the site, correct?

2 A. We were aware that the Web site existed between August
3 and December, 2014. We were aware of it. We were monitoring
4 it. We were not expending a significant amount of resources
5 on it during that time period.

6 Q. Then around December of 2014 you gathered information
7 that eventually led you to determine that the administrator
8 of the Web site was located at a residence in Naples,
9 Florida. Is that right?

10 A. That is correct.

11 Q. So you obtained a warrant to search that person's
12 residence?

13 A. That's correct.

14 Q. And that was just kind of a traditional residential
15 search; that didn't involve the NIT technology that we're
16 going to talk about in a minute, correct?

17 A. Correct.

18 Q. Now, you were personally present during the execution of
19 that Florida search warrant. Is that correct?

20 A. I was.

21 Q. And that began on February 19, 2015, correct?

22 A. That is correct.

23 Q. When you were searching that residence you saw a laptop
24 computer, correct?

25 A. I did.

—D. Alfin - Direct—

1 Q. The laptop computer appeared to be hosting the Playpen
2 site.

3 A. No.

4 Q. The home page was displayed on the --

5 MS. GRATTON: Objection, Your Honor. He's leading
6 the witness.

7 THE COURT: Well, he's --

8 MS. GRATTON: The witness can testify to what he
9 observed directly, if asked what he observed.

10 THE COURT: Well, I don't -- I'm not going to
11 restrict him from leading the witness under these
12 circumstances.

13 MR. GRINDROD: Thank you, Your Honor.

14 BY MR. GRINDROD:

15 Q. So you saw a laptop. You're familiar -- you were
16 familiar before you went to the Florida residence with what
17 the home page of the Playpen site looked like, correct?

18 A. Correct.

19 Q. And when you got to the Florida residence you saw a
20 laptop, and displayed on the screen of the laptop was what
21 you recognized to be the Playpen site, some part of it.

22 A. That is correct.

23 Q. I want to show you a couple photographs. Do you have an
24 exhibit binder in front of you, sir?

25 A. I do.

—D. Alfin - Direct—

1 Q. And I direct you to what's been marked as Defense
2 Exhibit 2.

3 A. I have the exhibit in front of me.

4 Q. And do you recognize what that is, sir?

5 A. I do.

6 Q. Can you tell the Court?

7 A. This is a photograph that was taken during the execution
8 of a search warrant at the residence of the administrator of
9 the Playpen Web site. This is a photograph of his laptop as
10 it was when we encountered it during the execution of that
11 warrant.

12 Q. And that's the execution in Naples, Florida, right?

13 A. That's correct.

14 Q. The one you were present at.

15 A. Correct.

16 Q. Now, can you turn to page 2 of that exhibit?

17 A. I have it in front of me.

18 Q. Okay. And that is the home page of the Playpen site as
19 it appeared on February 19th, 2015, correct?

20 A. No, this is the index page of the Web site that appears
21 after you log in to the Web site.

22 Q. I see. The border across the top of there, is that the
23 same on the home page as it is on the index page?

24 A. Could you be more specific?

25 Q. Sure. Let me do it this way:

—D. Alfin - Direct—

1 Can you turn to Exhibit 3 in that binder?

2 A. I have it in front of me.

3 Q. Is that a screenshot of the Playpen home page as it
4 appeared on the morning of February 20th, 2015?

5 A. I don't have it dated, but it does appear to represent
6 what the home page looked like on February 20th, 2015, yes.

7 Q. Okay.

8 THE COURT: So the search began on the 19th and
9 continued to the 20th.

10 THE WITNESS: Yes, Your Honor. We began execution
11 of the search warrant in Naples, Florida, the evening of
12 February 19th, and we eventually departed the subject's
13 residence the morning of February 20th, 2015.

14 BY MR. GRINDROD:

15 Q. Now, this same screenshot, Defense Exhibit 3, that was
16 what the home page looked like from February 20th through
17 February 27th, at least, correct?

18 A. That is correct.

19 Q. The warrant application in this case -- are you familiar
20 with that document?

21 A. I am familiar with that document.

22 Q. Okay. So you know that the warrant application said that
23 the home page showed, quote, "Two images depicting partially
24 clothed prepubescent females with their legs spread apart,"
25 unquote.

—D. Alfin - Direct—

1 A. The warrant application cited a specific date and time,
2 and it cited the image as it appeared on that specific date
3 and time, and that is an accurate description of the image
4 that appeared on that date and time.

5 Q. Okay. So let me ask you the question this way:

6 That quote I just read is exactly the quote that
7 appears in the warrant affidavit, correct?

8 A. In which warrant affidavit?

9 Q. The one for the NIT warrant.

10 A. Correct.

11 Q. And you would agree with me that the home page that is
12 shown on Defense Exhibit 3 does not display two prepubescent
13 females, correct?

14 A. It does not.

15 Q. It does not depict anyone with their legs spread apart,
16 correct?

17 A. It does not.

18 Q. Now, at the time you executed the Florida warrant back on
19 February 19th into the 20th you clearly saw the Web site at
20 that point, correct?

21 A. I did.

22 Q. And you clearly saw the new logo at that point, correct?

23 A. I saw it, but I did not notice it because it was an
24 insignificant and minor change to the Web site.

25 Q. So your testimony is that you did see the new logo,

—D. Alfin - Direct—

1 correct?

2 A. Yes. As I stated earlier, I saw the administrator's
3 laptop in his residence, and in that photograph the new logo
4 was present. So, yes, I did see it, and, as I stated
5 previously, it went unobserved by me because it was an
6 insignificant change to the Web site.

7 Q. So you saw it but it was unobserved.

8 A. Correct.

9 Q. After February 20th the FBI seized the server that hosted
10 the Playpen site, correct?

11 A. We seized the server hosting the Playpen Web site either
12 the evening of February 19th, 2015, or the early morning
13 hours of February 20th, 2015.

14 Q. And after you seized the Playpen site or the server for
15 the Playpen site the FBI continued to monitor the site,
16 correct?

17 A. We took a copy of the Web site, and we ran that copy of
18 the Web site from a government facility within the Eastern
19 District of Virginia. While we ran the Web site from the
20 Eastern District of Virginia, we did monitor activity on the
21 Web site.

22 Q. So the answer to my question is, yes, from February 20th
23 on, while the FBI was operating the Web site, you were also
24 monitoring the Web site, correct?

25 A. The answer to that question is yes.

—D. Alfin - Direct—

1 Q. Okay. So that would encompass the entire period from
2 February 20th through at least February 27th, correct?

3 A. It would.

4 Q. At no point between February 20th and February 27th,
5 2015, did the FBI submit a new warrant application to any
6 judge based on this new home page, correct?

7 A. We obtained one NIT warrant the morning of February 20th,
8 2015. That is the only NIT warrant that was obtained during
9 this investigation.

10 Q. Okay. So, then, let me ask you my question, because I
11 think the answer is no, but you can tell me.

12 So my question was that at no point did the FBI
13 submit a new warrant application based on the new change to
14 the Web site.

15 A. Sir, I need to correct an earlier statement.

16 There was a second application for a separate NIT
17 warrant. It was never executed or utilized, but it was not
18 related to the logo change. We did not submit a second NIT
19 warrant reflecting the logo change.

20 Q. But there was a second warrant obtained?

21 A. There was a second warrant obtained specific to an
22 individual user on the Web site. That warrant was never
23 executed.

24 Q. As far as you know, that second warrant was never used to
25 justify any search against Mr. Matish, correct?

—D. Alfin - Direct—

1 A. Correct.

2 Q. But when did you go back for the second warrant?

3 A. After February 20th, 2015.

4 Q. Was it before February 27th?

5 A. I don't recall the exact date.

6 Q. Did you go back to the same Magistrate Judge?

7 A. No, that second warrant was in front of a different
8 judge.

9 Q. But at some point after February 20th and before
10 February 27th the FBI did go get another warrant; they just
11 didn't update the warrant that they got in this case.

12 A. I don't know if it was before February 27th.

13 Q. But just to circle back to my original question --

14 THE COURT: Well, does this have any relevance?
15 Because it was never executed.

16 MR. GRINDROD: Well, Your Honor, I think --

17 THE COURT: It wasn't used in this case, so --

18 MR. GRINDROD: Right. I --

19 THE COURT: We seem to be spending a lot of time on
20 it.

21 MR. GRINDROD: I'll move on, Your Honor. I think I
22 got what I needed there.

23 BY MR. GRINDROD:

24 Q. So let's talk a little bit about the NIT. You're
25 familiar with this technology, correct?

—D. Alfin - Direct—

1 A. I am.

2 Q. And by "NIT" you understand me to be talking about the
3 N-I-T or the Network Investigative Technique?

4 A. Correct.

5 Q. Before the government obtained the NIT warrant in this
6 case, I think your testimony was that the FBI had already
7 seized the server that hosted the Playpen site, correct?

8 A. That is correct.

9 Q. But, from the FBI's perspective, the problem was that
10 even though the government had physical possession of that
11 server it couldn't identify the users, the people who were
12 logging on to the Playpen site. Fair?

13 A. That is correct.

14 Q. And that problem existed because Playpen users navigated
15 to the Playpen site through the Tor network, right?

16 A. That is correct.

17 Q. And Tor software protects users' privacy online by
18 bouncing communications off different computers all around
19 the world before the signal goes to the eventual destination,
20 right?

21 A. That is accurate.

22 Q. Tor prevents someone attempting to monitor an Internet
23 connection from learning what sites a user visits, correct?

24 A. That is correct.

25 Q. And it prevents the Web sites the user visits by learning

—D. Alfin - Direct—

1 the user's physical location.

2 A. That is correct.

3 Q. So even though you had the Playpen host server, you still
4 could not tell the physical location of the users accessing
5 the Playpen site.

6 A. That is correct.

7 Q. That's where the NIT comes in, right?

8 A. That is correct.

9 Q. So the NIT, the N-I-T --

10 THE COURT: Excuse me a minute.

11 You could determine their IP number, but you
12 couldn't determine the physical location of the computer just
13 from the IP number. Is that right?

14 THE WITNESS: No, Your Honor. The Tor software
15 allows an individual to host a Web site within the Tor
16 network, and when you do that that Web site is referred to as
17 a hidden service.

18 With a traditional Web site when a user accesses it
19 the Web site would maintain log files showing dates, times,
20 and IP addresses. When a user accesses one of these hidden
21 services on the Tor network their true IP address is
22 concealed. The actual Web site never sees their true IP
23 address, and the user also never sees the true IP address of
24 the server.

25 THE COURT: The IP address, is that different than

—D. Alfin - Direct—

1 the IP identification number?

2 THE WITNESS: No, Your Honor, those would reference
3 the same thing.

4 THE COURT: All right. Go ahead.

5 BY MR. GRINDROD:

6 Q. So let's break this down a little.

7 So you're operating the Playpen site, the FBI,
8 correct?

9 A. Correct.

10 Q. Someone logs on to the Playpen site. You can tell
11 without the NIT that someone has logged on, correct?

12 A. That is correct.

13 Q. But you don't know the IP address of the person who just
14 logged on, right?

15 A. That is correct.

16 Q. And you don't have any other identifying information,
17 like what software that computer is running or what the
18 person's logon name for their own operating system is. You
19 don't have any of that information, right?

20 A. We don't have that information.

21 Q. So before you deploy the NIT, when someone logs on to the
22 Playpen site you don't know their IP address, any identifying
23 information, or the physical location of the computer that
24 just logged on, right?

25 A. We do not know any of the specific items that you listed.

—D. Alfin - Direct—

1 Q. And when we say you don't know the location of the
2 computer, because you don't have the IP address or any other
3 information you don't know -- you have no idea where that
4 computer is located, right? In other words, let me say it
5 this way:

6 It's not as if you know that it's in some city but
7 you can't get the street address, correct? That computer
8 could be located anywhere in the world.

9 A. That is correct.

10 Q. Okay. And before you deploy the NIT there's no way that
11 you can tell where in the world that computer logging on
12 might be located.

13 A. In general, that is correct.

14 Q. So the NIT is computer code, right?

15 A. It is a set of computer instructions or computer code,
16 yes.

17 Q. Is it fair to say we can kind of think of this like a
18 package of data or code?

19 A. The NIT is a set of very simple computer instructions
20 that, when executed, instruct a computer to send to the
21 government, in this investigation to a computer under the
22 government's control within the Eastern District of Virginia,
23 several pieces of identifying information.

24 Q. Thanks. Let me try to break that down step-wise a little
25 bit.

—D. Alfin - Direct—

1 So someone logs on to, in this case, the Playpen
2 site. When you deploy the NIT, the FBI is sending to the
3 person's computer who just logged on some set of code or
4 data, correct?

5 A. The way that you've described it is not technically
6 accurate and is not reflected in the NIT warrant.

7 The way that the NIT works is the software is
8 installed on the server in the Eastern District of Virginia.
9 After a user of the Playpen Web site takes certain actions,
10 including downloading information from the server in the
11 Eastern District of Virginia, that information is
12 supplemented with the NIT instructions. So the user
13 downloads the NIT to their computer and takes it to their
14 computer, wherever it may be located.

15 Q. Now, you say that the user downloads this information.
16 They don't know that they're downloading this information,
17 right?

18 A. That's correct.

19 Q. The whole point of the NIT is that this extra package of
20 data that you're sending to the activating computer is
21 invisible, right?

22 A. The data that the activating computer is downloading is
23 intended not to be observed by the user, that's correct.

24 Q. And when you talk about the information that the user's
25 computer is downloading, you're talking about after you click

—D. Alfin - Direct—

1 through the home page the next screen would appear, correct?

2 Like it takes you to the table of contents, right?

3 A. After you log in to the Web site with a user name and
4 password you would arrive at the table of contents.

5 Q. And, so, when you refer to the information that the user
6 is downloading you mean the computer code that will make the
7 table of contents appear on their screen, right?

8 A. No.

9 Q. Well, what do you mean by that?

10 A. The way that the NIT was deployed in this investigation,
11 a user had to take several affirmative actions before they
12 would download the NIT to their computer.

13 In the matter at hand the user logged in to the
14 Playpen Web site with a user name and password, they arrived
15 at the index site, they went to the bestiality section of
16 Playpen. At that point they --

17 Q. But --

18 THE COURT: Well, wait a minute. If you ask him a
19 question, let him answer it.

20 MR. GRINDROD: Sorry.

21 BY MR. GRINDROD:

22 Q. Okay. Go ahead.

23 A. After the user went to the bestiality section of Playpen,
24 the section of the Web site that advertised prepubescent
25 children engaged in sexual activities with animals, a user

—D. Alfin - Direct—

1 observed that one post was titled something to the effect of
2 "Girl 11YO," meaning years old, "with dog." The user then
3 clicked on that post to open it. At that point that user
4 downloaded several images of child pornography and the NIT
5 instructions to their computer.

6 Those are the steps that were taken for the NIT to
7 be deployed in this investigation.

8 Q. Okay. So let's break this down, because I think we're
9 talking about two different things.

10 I'm asking what the warrant authorized.

11 A. Okay. That's not what you asked me.

12 Q. So let me make that clear, because -- so the warrant
13 mentioned that the FBI had the ability to narrow the
14 situations in which they would deploy the NIT, right? That
15 was in footnote 8 of the NIT affidavit.

16 A. I can't cite the specific paragraph, but the warrant did
17 say that we may restrict how we deploy the NIT, yes.

18 Q. The way you deployed it is much narrower than what the
19 warrant authorized, correct?

20 A. That is correct. The warrant authorized us to deploy the
21 NIT against anyone who logged in to Playpen with a user name
22 and password, because after doing so there is probable cause
23 to believe that someone having done this is attempting to
24 access, download, receive, or distribute child pornography.

25 Q. Okay. So I'm going to ask you questions that contemplate

—D. Alfin - Direct—

1 that situation that is set out in the warrant, rather than
2 any specific execution that you referenced in your earlier
3 response, okay?

4 A. I will answer your questions.

5 Q. So someone logs on to the Playpen Web site by entering a
6 user name and password, correct?

7 A. Yes.

8 Q. They have to click "Okay" or "Login." Is that correct?

9 A. I don't remember exactly what the button says, but they
10 enter their user name, they enter their password, and then
11 they log in to the Web site.

12 Q. And under the NIT warrant, at that point the FBI is
13 authorized to deploy the NIT to search that logging-in
14 computer.

15 A. Yes.

16 Q. And when you talk about the code going back to that
17 logging-in computer, the activating computer or user's
18 computer, it's a physical package of data, computer code,
19 that travels to the activating computer, correct?

20 A. I would not refer to computer code as a physical item.
21 It is computer code.

22 Q. And it's transmitted physically, right?

23 A. Digitally. I mean, it is computer code.

24 Q. Computer code. And, so, is it a fair analogy to say
25 that, basically, this code is kind of like installed onto the

—D. Alfin - Direct—

1 activating computer?

2 A. No, the NIT is not installed onto the computer, nor does
3 it make any permanent changes to the computer, nor are there
4 any remnants of it left behind after it executes the limited
5 set of instructions authorized by the NIT warrant.

6 Q. So a computer code works by telling a computer what to
7 do, right, basically?

8 A. That's fair.

9 Q. And in this case the NIT code was sent to the activating
10 computer, went onto that activating computer and told that
11 computer what to do, right?

12 A. After the activating computer downloaded the NIT
13 instructions, those instructions were run. The computer
14 executed those instructions, and then there was nothing left
15 behind, no pieces of the NIT or anything like that, on the
16 computer.

17 Q. But -- I think you answered my question.

18 When we talk about the information being gathered by
19 the NIT, this information included the IP address, correct?

20 A. After the NIT executed the instructions on the computer,
21 it transmitted information to a government server in the
22 Eastern District of Virginia. In transmitting that data, the
23 IP address of the activating computer is observed and
24 captured.

25 Q. And the NIT also gathered other information that was

—D. Alfin - Direct—

1 stored on the activating computer, like the host's name and
2 the logon name, correct?

3 A. That is correct.

4 Q. And it took this information that it gathered from the
5 activating computer and sent it to the FBI.

6 A. That is fair.

7 Q. Okay. So I started this conversation about the NIT by
8 talking about kind of problem and solution, right? The
9 problem was, from the FBI's standpoint--

10 THE COURT: All right. Let me ask something.

11 So the NIT sent back to the FBI the IP address.

12 THE WITNESS: Yes, Your Honor.

13 THE COURT: And what did that tell you?

14 THE WITNESS: It told us the true IP address of the
15 user who accessed the Web site, which prior to execution of
16 the NIT instructions, because of the way the Tor network
17 functions, we were unable to see the true IP address of the
18 user's computer.

19 THE COURT: All right. Well what does the IP
20 address give you? Does it give you just the ID number of the
21 computer, or does it give you the location of the computer?
22 What does it give you?

23 THE WITNESS: With the IP address we are able to use
24 the IP address and send a subpoena to an Internet service
25 provider and ask them to identify the subscriber who had that

—D. Alfin - Direct—

1 IP address on that date and time.

2 THE COURT: So that allowed you to trace the
3 location of that computer.

4 THE WITNESS: Yes, Your Honor.

5 THE COURT: And you say it also included the host's
6 name.

7 THE WITNESS: Yes, Your Honor, that's --

8 THE COURT: Is the host Playpen?

9 THE WITNESS: No, Your Honor, that would be the host
10 name of the user's computer. When you install an operating
11 system on your computer it will typically ask you what do you
12 want your computer name to be, and that is the name.

13 THE COURT: So you mean the host of the computer
14 whose IP address you had.

15 THE WITNESS: Yes.

16 THE COURT: And also the login name.

17 THE WITNESS: Yes, Your Honor, in this case it would
18 be a Windows operating system user name.

19 THE COURT: Okay.

20 BY MR. GRINDROD:

21 Q. Let me direct you, Agent Alfin, to what's in your binder
22 marked as Defense Exhibit 5.

23 MR. GRINDROD: Your Honor, this exhibit was part of
24 information that was provided by the government and is
25 covered by the protective order in this case, so I would ask

—D. Alfin - Direct—

1 that if the Court is going to admit this evidence that it be
2 filed under seal.

3 THE COURT: Are you asking me to admit it?

4 MR. GRINDROD: Not at this point, Your Honor.

5 THE COURT: All right. Well, ask the question,
6 then.

7 MR. GRINDROD: All right. Thank you, Your Honor.

8 BY MR. GRINDROD:

9 Q. Are you familiar with this kind of document, Agent Alfin?

10 A. I am.

11 Q. Can you tell the Court what it is?

12 A. This is a user report, or a page from a user report, that
13 my unit generated at the conclusion of our investigation. It
14 shows specific activities, specific actions, attributed to
15 specific users of the Playpen Web site. It is called a
16 Cygnus report, Your Honor.

17 THE COURT: It's called a what?

18 THE WITNESS: Cygnus report, Your Honor.

19 Cygnus, C-Y-G-N-U-S. It's not an acronym, it's just
20 named after a constellation.

21 THE COURT: Okay.

22 BY MR. GRINDROD:

23 Q. So this is a document that's produced by law enforcement,
24 correct?

25 A. Correct.

—D. Alfin - Direct—

1 Q. And basically what this is is a way of displaying the
2 information that was gathered when the NIT was deployed
3 against a user, correct?

4 A. This specific page of the report contains information
5 that was identified by a NIT, yes.

6 Q. All right. And your clarification -- there are a number
7 of tabs at the top, right?

8 A. There are.

9 Q. And so before I took this screenshot you would agree that
10 it appears that I clicked on the tab that would display the
11 NIT hits. Is that right?

12 A. Yes, that's correct.

13 Q. So the full Cygnus report contains more information than
14 just this page, correct?

15 A. That is correct.

16 Q. So I want to direct your attention to a couple pieces of
17 information that are displayed here.

18 First, all the way to the left it says, "Date/Time,"
19 and it says, "2015-02-27." Does that indicate that this
20 information is relating to the deployment of the NIT on that
21 day?

22 A. Yes. This reflects information that was identified by a
23 NIT on February 27th, 2015.

24 Q. And this was the NIT deployment against Mr. Matish's
25 computer, correct?

—D. Alfin - Direct—

1 A. That is correct.

2 Q. And some of the information on here was gathered from his
3 computer by the NIT and sent back to the FBI, correct?

4 A. That is correct.

5 Q. That information includes the IP address?

6 A. I want to clarify. With the IP address, that was not
7 actually resident on his computer. After the NIT collected
8 information it sent it over the regular Internet to our
9 server, and his IP address was observed at that time.

10 Q. Okay. And the MAC --

11 A. That is the MAC address of the computer.

12 MAC is an acronym for Media Address Control. It is
13 a unique hardware identifier on an individual's network card.
14 For example, if they're using a hard-wired Internet cable,
15 that port on the computer where you plug it into will have a
16 unique MAC address, or a wireless card will also have a
17 unique MAC address.

18 Q. And, so, the purpose of gathering that information is
19 because multiple computers can be logged on to the Internet
20 through the same IP address, right?

21 A. That is correct.

22 Q. And, so, the reason the FBI collected that information
23 and some other information we're going to talk about is
24 because it would help the FBI narrow the possible computers
25 who might have been logging on to the site from that IP

—D. Alfin - Direct—

1 address, correct?

2 A. You could use the MAC address to identify which computer
3 in a residence was the one that logged on to the Web site.

4 Q. So if I have three laptops in my house and four cell
5 phones that connect to Wi-Fi, just based on the IP address
6 the FBI may not be able to tell which device actually logged
7 on to Playpen, correct?

8 A. That's possible.

9 Q. But because the FBI gathered from the activating computer
10 this additional information, it can help the FBI pinpoint
11 which device actually logged on.

12 A. That would be one way of identifying the device.

13 Q. And another way of identifying the device would be based
14 on the host name.

15 A. That's correct.

16 Q. That's other information that the NIT gathered from, in
17 this case, Mr. Matish's computer and sent back to the FBI.

18 A. That is correct.

19 Q. The same with the login name. Here that says, "Eddie,"
20 correct?

21 A. It does.

22 Q. And, so, a login name, at least with the Windows
23 operating system, is created by whoever installs the Windows
24 operator system on their computer, correct?

25 A. Generally, yes.

—D. Alfin - Direct—

1 Q. And sometimes different members of the family may have
2 different login names for different people, correct?

3 A. That is generally correct.

4 Q. Different people who use that same computer, correct?

5 A. Yes.

6 Q. So that information helped the FBI identify not only the
7 actual device that was logging on to Playpen but also perhaps
8 helped the FBI identify the specific person who was using
9 that device or specific account that was associated with that
10 device that logged on to Playpen, correct?

11 A. This information could be used to identify a specific
12 device.

13 Q. And that information, like the other information we're
14 talking about, is gathered from Mr. Matish's computer, sent
15 back to the FBI, and that's how it ended up in the Cygnus
16 report.

17 A. That's correct.

18 Q. All this information gathered by the NIT pursuant to the
19 NIT warrant.

20 A. Correct.

21 Q. And the last piece of information here that falls into
22 that category is the entry under "OS," correct?

23 A. Correct.

24 Q. "OS" is operating system?

25 A. Correct.

—D. Alfin - Direct —

1 Q. And, so, this information indicates that the operating
2 system that accessed the Playpen site -- or the operating
3 system that was running on the computer that accessed the
4 computer site was a Windows operating system.

5 A. That's correct.

6 Q. So, again, if there was a MAC, a Windows program,
7 operating system, in somebody's house, this might help you
8 say, we think it was the computer that's running Windows, not
9 the MAC.

10 A. That is possible, yes.

11 MR. GRINDROD: Your Honor, I offer at this point
12 Defense Exhibit 5, under seal.

13 THE COURT: All right. Why should it be under seal?

14 MR. GRINDROD: I have it no objection to it being --

15 THE COURT: Well, I'm asking the government.

16 MS. GRATTON: The Cygnus report was provided
17 pursuant to the agreed discovery protective order. The
18 report itself contains a wide amount of information related
19 to the Playpen site, including information related to this
20 defendant and several other targets. And, so, the report was
21 provided, as the parties agreed, pursuant to the protective
22 order, which would require any portion of its filing under
23 seal.

24 THE COURT: All right. The Court will admit the
25 exhibit with the proviso that it be placed under seal,

—D. Alfin - Direct—

1 meaning that it will not be a public document.

2 (The exhibit was admitted into evidence under seal.)

3 BY MR. GRINDROD:

4 Q. And, Agent Alfin, before we move away from that document,
5 this is probably obvious, but the notation on the bottom of
6 that page says, "Subject to protective order under seal."
7 That's obviously, not something that would show up on the
8 Cygnus report, correct? That was something added by the
9 lawyers?

10 A. That is correct.

11 MR. GRINDROD: Your Honor, I also offer Defense
12 Exhibits 2 and 3.

13 I would note that I believe Defense Exhibit 3 was
14 attached to some of the motions and responses in this case.

15 THE COURT: All right. Exhibits 2, 3, and 5 will be
16 admitted, with the sealed proviso as to Number 5.

17 (The exhibits were admitted into evidence.)

18 BY MR. GRINDROD:

19 Q. So, Agent Alfin, when we started talking about the NIT we
20 talked about it in terms of a problem and a solution, the
21 problem being that, from the FBI's standpoint, you couldn't
22 identify the physical location or any identifying information
23 about the computer that was logging in to the Playpen site,
24 correct?

25 A. Correct.

—D. Alfin - Direct—

1 Q. And the NIT was a way of gathering that information.

2 A. Yes.

3 Q. So if the problem was that you didn't know the location
4 of the activating computer -- this may be obvious, but before
5 you search the user's computer with the NIT you don't know
6 where that computer is located, right?

7 A. Correct.

8 THE COURT: We went through that before, didn't we,
9 Counsel?

10 MR. GRINDROD: Okay.

11 BY MR. GRINDROD:

12 Q. So here in this case the NIT warrant authorized the FBI
13 to search any user or administrator who logged on to the
14 Playpen Web site, correct?

15 A. The warrant that was obtained here in the Eastern
16 District of Virginia did authorize us to utilize the NIT
17 against any user's computer after that user logged in to the
18 Web site with a user name and a password.

19 Q. If you could, imagine for me that the NIT warrant instead
20 said that you could only search the computer of a user if
21 that computer was located in the Eastern District of
22 Virginia.

23 A. I'm imagining it.

24 Q. Okay. With this technology that you used in this case
25 you could not -- you couldn't do that, right?

D. Alfin - Cross

1 A. As stated previously, the NIT was utilized because we did
2 not know the physical location of a computer before the NIT
3 was utilized.

4 MR. GRINDROD: I have no further questions -- may I
5 consult with counsel for one moment, Your Honor?

6 (There was a pause in the proceedings.)

7 MR. GRINDROD: I have no further questions at this
8 time.

CROSS-EXAMINATION

9
10 BY MS. GRATTON:

11 Q. Good afternoon.

12 A. Good afternoon.

13 Q. Can I have you look at what's marked in that binder as
14 Defendant's Exhibit 4.

15 A. I have it in front of me.

16 Q. What does that depict?

17 A. This is the home page of the Playpen Web site prior to
18 February 19th, 2015.

19 Q. Is there a date depicted anywhere on that exhibit?

20 A. In the bottom right-hand corner it indicates that this is
21 how the Web site appeared on or about February 3rd, 2015.

22 Q. Are you familiar with the circumstances under which this
23 image was captured?

24 A. I am. An undercover FBI agent operating from my office
25 in the Linthicum, Maryland area accessed the Playpen Web site

D. Alfin - Cross

1 on February 3rd, 2015, and took several screenshots of the
2 Web site. This was one of them.

3 Q. And can you describe what's been referred to as the logo
4 located up in the left-hand corner?

5 A. The logo on the top left of this page has the word
6 "Playpen," and on either side of the logo there are two
7 prepubescent females, wearing what appear to be underwear or
8 bathing suits, with their legs spread.

9 Under that is the text that says, "No cross-board
10 reposts, 7Z preferred, encrypt file name, include preview,
11 peace out."

12 Q. And if you could turn, then, back to Defendant's
13 Exhibit 3, which has already been admitted.

14 Can you describe the difference and the similarities
15 in that logo to the one in the other?

16 A. The old logo depicted two prepubescent females. The new
17 logo depicts a single prepubescent female wearing fishnet
18 stockings and posed in a sexually suggestive manner.

19 Q. In all other respects, the text you just described, is
20 that the same?

21 A. Correct, with the addition of the words "welcomes you."

22 Q. Have you had the opportunity to review this login page,
23 both with the former logo and the new logo?

24 A. Yes, I have.

25 Q. Is the process for logging in the same?

D. Alfin - Cross

1 A. It is.

2 Q. Does it take you to the same place?

3 A. It does.

4 Q. Is the content the same?

5 A. It is.

6 Q. In any other aspect beyond the photo, was the content of
7 Playpen different after February 19th?

8 A. No, it was still the same Web site that it was prior to
9 February 19th.

10 Q. And you discussed the photos of the administrator's
11 laptop as they appeared during the execution of the search
12 warrant at his home in Naples, Florida, beginning on
13 February 19th?

14 A. Yes.

15 Q. When did that search conclude?

16 A. That search concluded the morning of February 20th, 2015.

17 Q. I believe you testified that you saw the laptop; that the
18 logo was present on it but it went unobserved by you.

19 A. That is correct.

20 Q. Did you communicate with the warrant affiant concerning
21 the appearance of the Web site before the NIT warrant was
22 obtained?

23 A. No, I did not.

24 Q. There's been a number of references to passing through
25 the home page or clicking through the home page. Can you

D. Alfin - Cross

1 describe in detail how one gets from this home page into the
2 content of Playpen?

3 A. Prior to logging in to the Playpen Web site, a user would
4 have to click on one of the -- excuse me -- click on the link
5 in the middle of the page that says, "Register an account
6 with Playpen."

7 After doing that they would be taken to a separate
8 page with the instructions on creating an account on the
9 Playpen Web site, including instructions such as entering
10 fake e-mail addresses and making sure that you don't do
11 anything that could be used to identify you.

12 At that point the user would select a user name and
13 a password, and after that they would be redirected back into
14 this login page, and they would have to enter that user name
15 and password, and then they would be able to log in to the
16 Web site.

17 Q. And that, you're describing, is the registration process
18 for creating a Playpen account.

19 A. That's correct.

20 Q. What's the process once a person has an account?

21 A. After a person has an account, they just need to come to
22 this front page, enter their user name and password, and then
23 they can log in to the Web site.

24 Q. But in order to get there they have to have gone through
25 the registration process, as you just testified.

D. Alfin - Cross

1 A. Correct.

2 MS. GRATTON: One moment.

3 (There was a pause in the proceedings.)

4 MS. GRATTON: Before we move on, Your Honor, I would
5 move to admit what's been marked as Defendant's Exhibit 4.

6 MR. GRINDROD: No objection.

7 THE COURT: All right. Exhibit 4 will be admitted.

8 (The exhibit was admitted in evidence.)

9 THE COURT: Would you give me the steps again for
10 registering for the Web site?

11 THE WITNESS: After you come to the main page of the
12 Web site, Your Honor, as it's depicted --

13 THE COURT: How do you get to the main page of the
14 Web site?

15 THE WITNESS: The Playpen Web site existed on the
16 Tor network, so you can't just use a normal Internet browser
17 to get there. Commonly, on a user's computer you may have
18 Internet Explorer or Firefox or something of that nature.
19 Those web browsers will not be able to connect you to the
20 Playpen Web site.

21 Similarly, you would not be able to go to Google and
22 find the Playpen Web site. You would have to first download
23 specialized software, generally the Tor browser, which is a
24 special web browser that --

25 THE COURT: The what browser?

D. Alfin - Cross

1 THE WITNESS: Tor browser, Your Honor.

2 THE COURT: Tor? Okay.

3 THE WITNESS: It allows you to both connect to the
4 regular Internet and hide where you're coming from. It also
5 allows you to connect to Web sites, like Playpen, that exist
6 only within the Tor network.

7 THE COURT: Well, how does one know about the Tor
8 network?

9 THE WITNESS: The Tor network itself is freely
10 available. It can be used for a variety of purposes. Not
11 all of them are illegal. There is --

12 THE COURT: Well, is the Tor network advertised
13 anywhere? How does anybody know that it exists?

14 THE WITNESS: It has a Web site on the regular
15 Internet that advertises it. There are a number of
16 organizations that advocate its use for various reasons.
17 It's gotten a significant amount of press coverage in the
18 past several years, so it would not be uncommon for someone
19 to know about the Tor network in general.

20 THE COURT: All right. So once you know that there
21 is a Tor network, what do you have to do to log on to that
22 network?

23 THE WITNESS: First you would have to download the
24 special software, the Web browser, that would allow you to
25 connect to the Tor network.

D. Alfin - Cross

1 THE COURT: Where would you get that?

2 THE WITNESS: From the Tor Project Web site. It's
3 a --

4 THE COURT: So you would have to go to the Tor Web
5 site?

6 THE WITNESS: Yes, Your Honor.

7 THE COURT: That would be step one?

8 THE WITNESS: Yes, Your Honor.

9 THE COURT: And how do you do that? I mean, is that
10 like going to any other Web site?

11 THE WITNESS: Yes, Your Honor. The Tor Web site
12 exists on the regular Internet, as most other Web sites do.
13 From there you can read information about the Tor network,
14 and you can also download the Tor browser that will allow you
15 to connect to the Tor network.

16 THE COURT: Once you connect to the network, then
17 you have to register with Tor.

18 THE WITNESS: After you connect to the Tor network
19 you're immediately on the Tor network. The network itself
20 does not require any special registration. This particular
21 Web site, Playpen, did require registration, but you wouldn't
22 be able to find the Playpen Web site without taking several
23 other steps as well.

24 BY MS. GRATTON:

25 Q. Could you perhaps describe those steps for the Court?

D. Alfin - Cross

1 THE COURT: Well, how would you know what steps to
2 take?

3 THE WITNESS: So typically if you're looking for
4 something on the regular Internet you could go to Google, you
5 could type in that thing, and you would find a Web site on
6 the topic that you're looking for.

7 With the Tor network there are various index Web
8 sites that function in a somewhat similar manner, but they
9 don't function like search Web sites on the regular Internet
10 do. For example, there are a number of index Web sites that
11 exist within the Tor network that show you links to various
12 child pornography Web sites. In the case of Playpen, it was
13 listed on at least two Web sites whose purpose was listing
14 child porn Web sites within the Tor network.

15 So first you would go to one of these index Web
16 sites, and then from there you would find the link to the
17 child porn Web site, such as Playpen, and you would click on
18 it from there, and then you would be brought to this front
19 page of the Playpen Web site.

20 THE COURT: There seems to be some dispute between
21 the government and the defense as to whether someone could
22 accidentally stumble on Playpen or Tor.

23 THE WITNESS: It would be incredibly unlikely for
24 someone to accidentally stumble upon the Playpen Web site,
25 but the Tor network itself is not illegal. You can use the

D. Alfin - Cross

1 Tor network to do legal things. However, finding your way to
2 a Web site like Playpen takes several affirmative steps by
3 the user, and it is highly unlikely that someone who is not
4 searching for child pornography would find their way to the
5 Playpen Web site.

6 THE COURT: When you were investigating the content
7 of the Web site did you ever determine the origin of the
8 pornography that was on the Web site; that is, whether it
9 became from overseas or --

10 THE WITNESS: I reviewed the content of the Web site
11 on multiple occasions. Of the child pornography that we were
12 able to recover and analyze from the Web site, there were
13 hundreds of identified victims. Some of them were domestic,
14 from previous law enforcement investigations within the
15 United States; some of them were victims that were identified
16 overseas by foreign law enforcement investigations.

17 THE COURT: Do you have any concept of whether most
18 of it was foreign or domestic?

19 THE WITNESS: I don't know the answer to that, Your
20 Honor.

21 THE COURT: It was a combination of the two?

22 THE WITNESS: Yes, Your Honor.

23 BY MS. GRATTON:

24 Q. If I may ask a follow-up point on that, were there
25 specific forums within Playpen's content that specified

D. Alfin - Cross

1 content available in different languages?

2 A. Yes. There were foreign language sections of Playpen
3 that advertised images and videos of children from foreign
4 countries, as well as offered an opportunity for users who
5 spoke those foreign languages to post child pornography and
6 discuss said topic with other users who spoke the same
7 language. The majority of users on the Playpen Web site who
8 posted content posted it in English.

9 Q. Did your investigation identify anyone utilizing the
10 Playpen network who had produced child pornography?

11 A. Yes, we identified a number of producers of child
12 pornography through the investigation of Playpen.

13 Q. Suffice to say that the content on that Web site
14 reflected a wide variety of child pornography from various
15 sources.

16 A. That is correct.

17 THE COURT: Foreign and domestic?

18 THE WITNESS: Yes, Your Honor. We have identified a
19 number of victims and hands-on offenders of children, both
20 domestically and internationally.

21 THE COURT: And you say there was also a process for
22 sharing?

23 THE WITNESS: Yes, Your Honor.

24 THE COURT: How did that work?

25 THE WITNESS: The Web site was set up into various

D. Alfin - Cross

1 categories. For example, there was a video section, and
2 within that video section there was a forum for preteen
3 videos - girls, there was a section for preteen videos -
4 boys. And, so, a user would go -- if they wanted to share
5 videos of girls, they would go to the preteen videos - girls
6 section, and within that section of the Web site they would
7 create a new topic, and they would upload images or videos of
8 child pornography that other users could then open that topic
9 and download those images and videos.

10 THE COURT: All right.

11 THE WITNESS: And that was the primary purpose and
12 use of the Web site.

13 BY MS. GRATTON:

14 Q. You mentioned in your testimony on direct a clarification
15 that the IP address doesn't come from a user's computer.

16 Where does it come from?

17 A. The IP address is generally assigned by the Internet
18 service provider to a user's modem. While the NIT transmits
19 its information to the government that IP address is
20 transmitted along with that information, just in the course
21 of how communications occur over the Internet.

22 Q. And the warrant authorized the government to retain that
23 information --

24 A. Correct.

25 Q. -- as part of that transmission.

D. Alfin - Cross

1 A. Correct.

2 Q. And you testified that the Tor network operates to mask
3 the IP address of a user. Can you explain that process?

4 A. The Tor network has two primary purposes. The first is
5 to allow a user to access the regular Internet and do so in
6 an anonymous fashion. So a user would go to the Tor Project
7 Web site, they would download the Tor browser, and then they
8 would use it to connect to normal Internet Web sites as they
9 normally would.

10 They could go to Google, or they could go to
11 cnn.com. They could access any Web site like they normally
12 would. The difference is that their communication -- instead
13 of going, essentially, directly from their computer to the
14 Google Web site, their Internet traffic is instead routed
15 across multiple computers around the world. And, so, you
16 still access the Google Web site, but the Google Web site
17 doesn't know where you are. It doesn't know if you're in
18 Virginia or if you're in a foreign country. And that's how
19 the majority of the users utilize the Tor network, just to
20 access the normal Internet.

21 The second primary purpose of the Tor network is
22 hidden services. Hidden services such as the Playpen Web
23 site are Web sites that exist only within the Tor network.
24 You cannot use your normal Internet browser to access them,
25 you need to download special software. And, so, when you do

D. Alfin - Cross

1 that you are affording benefits to both those users of those
2 Web sites and the people hosting those Web sites.

3 As a user of a Tor hidden service, when I connect to
4 the Tor hidden service the operator of the Web site doesn't
5 know where I am. They can't see my real IP address, and they
6 cannot identify me. Additionally, my communications are
7 encrypted, so law enforcement could not monitor my home
8 Internet connection, if they knew who I was, and see what I
9 was doing. They wouldn't be able to see what Web site I was
10 going to. They wouldn't be able to tell that I was logging
11 in to Playpen. So Tor hidden services protect the users in
12 that you cannot identify who the users are.

13 The second benefit of using a Tor hidden service is
14 that the person hosting the Web site is afforded similar
15 protections. If I host a Tor hidden service anyone is free
16 to connect to it, but even though they're connecting to my
17 Web site, even though they're logging in to my Web site, they
18 still don't know where my Web site is.

19 On the traditional Internet you can look up any Web
20 site you want to, such as google.com, and you can see exactly
21 where it's hosted, you can see its real IP address, you can
22 see what state it's in or what country it's in. You cannot
23 do that with a Tor hidden service. You cannot look up its
24 true IP address, you cannot immediately tell what country
25 it's in, what state it's in. None of that information is

D. Alfin - Cross

1 available to any third-party observers.

2 So Tor hidden services protect and offer anonymity
3 to both its users and to the people hosting the Tor hidden
4 services.

5 THE COURT: Well, now, what do you mean its user and
6 the people hosting them? What's the difference between a
7 user and the people hosting it?

8 THE WITNESS: So the individual in Naples, Florida
9 is the person who created and hosted the Playpen Web site.
10 He was the primary administrator; he created the Web site
11 himself. So he was the individual who was responsible for
12 creating these Web pages and making it available to users.

13 And then other individuals, such as the defendant in
14 this investigation, was just a user of the Web site, so he
15 would access it, log in to it, and consume the contents on
16 the Web site.

17 THE COURT: Well, when you register with Tor you
18 talked about going through a series of servers all over the
19 world.

20 THE WITNESS: Yes, Your Honor.

21 THE COURT: Do you have any idea how many servers
22 there are?

23 THE WITNESS: There are over a thousand servers,
24 Your Honor. They are actually publicly listed on the Tor Web
25 site. You can see exactly where they are and what their IP

D. Alfin - Cross

1 addresses are.

2 THE COURT: Well, then, how are they secure? How do
3 they secure the anonymity of the host and the users?

4 THE WITNESS: Because of the way a user connects to
5 the Tor network, every time they connect to the network they
6 establish a new circuit of those random servers around the
7 world, and that circuit changes --

8 THE COURT: You say "random"?

9 THE WITNESS: Yes, Your Honor. So it picks from
10 that list of over a thousand servers and says, for today I'm
11 going to route my communications through these three random
12 servers around the world. And those servers -- even though
13 we know where they are, all of those communications are
14 encrypted. So even if we were to monitor those servers, we
15 still would not be able to tell what communications are
16 passing through it, and we would not be able to identify who
17 the users of the Tor network were at that time.

18 BY MS. GRATTON:

19 Q. As part of that process, the routing through either from
20 the user to the Web site or the hidden service or the hidden
21 service back to the user, are the real IP addresses disclosed
22 to someone?

23 A. Yes. When a user connects to the Tor network they are
24 disclosing their real IP address to the first Tor node or
25 computer that they connect to.

—D. Alfin - Cross—

1 Q. So that is information that is disclosed in the process.

2 A. Yes.

3 Q. Can they prevent that disclosure through using the Tor
4 network?

5 A. No.

6 Q. I want to just briefly touch on the NIT in this case.
7 There's been a lot of discussion about searches and
8 deployments to user computers.

9 You described the NIT as computer instructions.

10 A. Yes.

11 Q. Where were those computer instructions installed after
12 the NIT warrant issued?

13 A. They were installed on a government-controlled server in
14 the Eastern District of Virginia.

15 Q. Did the FBI install them on any other computers or
16 locations?

17 A. The FBI configured the server such that when users
18 attempted to access the content of the Playpen Web site, in
19 addition to downloading that content, the NIT instructions
20 were added to that content. And, so, a user, by taking
21 several affirmative actions, ended up downloading that code
22 to their computer.

23 Q. So the code was included in the content that the user
24 requested?

25 A. Correct.

—D. Alfin - Redirect—

1 Q. And through -- when content is requested from a Web site,
2 how does it get to the user? Can you describe that process?

3 A. Generally, when a user connects to a Web site they will
4 initiate a connection to the Web site, and there will be,
5 essentially, a flow of communication going back and forth
6 between the user's computer and the Web site. The user's
7 computer will say, I want this piece of information, and the
8 Web site will say, here you go, and that exchange will
9 continue on and on until the user disconnects from the Web
10 site.

11 Q. So the information sent is the information requested.

12 A. Correct.

13 Q. In this case, Playpen content, including the NIT.

14 A. Correct.

15 Q. If Playpen had received no logins, no user requests,
16 would the NIT have left the server in the Eastern District of
17 Virginia?

18 A. No.

19 MS. GRATTON: I don't have any further questions,
20 unless -- no.

21 MR. GRINDROD: May I inquire, Your Honor?

22 THE COURT: You may.

23 REDIRECT EXAMINATION

24 BY MR. GRINDROD:

25 Q. I want to talk a little bit about the Tor network.

—D. Alfin - Redirect—

1 So the Tor network is not, for lack of a better word,
2 a bad thing in this case, necessarily, right?

3 A. Well, in this case it's a terrible thing. It was used to
4 host the world's largest child pornography Web site.

5 Q. Okay. People -- innocent -- there are a number of
6 innocent uses of the Tor network, correct?

7 A. Yes. I stated previously that you can use the Tor
8 network for legal purposes.

9 Q. In fact, the Tor Project is a nonprofit organization,
10 correct?

11 A. That's correct.

12 Q. And it was initially started by the United States Naval
13 Research Laboratory, right?

14 A. Tor Research was initially started by the United States
15 Naval Research Laboratory.

16 Q. And then it became a nonprofit, and a number of civil
17 liberties nonprofits provided funding to host the Tor
18 network, correct?

19 A. The majority of the Tor Project's funding comes from the
20 United States Government. Other funding comes from other
21 areas.

22 Q. So the United States Government is a primary funder of
23 Tor?

24 A. I believe that is still accurate, yes.

25 Q. And then a number of other nonprofit and philanthropic

—D. Alfin - Redirect—

1 organizations provide additional funding, correct?

2 A. I don't know exactly who the other organizations are, but
3 I do know that a number of other organizations fund it, yes.

4 Q. And one of the organizations that in the past has
5 provided funding to Tor is the Electronic Frontier
6 Foundation, an amicus in this case, correct?

7 A. I believe that's true.

8 Q. And people all over the world use Tor as a way of
9 protecting their privacy, right?

10 A. That is what the Tor Project claims, and I believe that
11 is correct.

12 Q. And as far as usage goes, some reports, as recently as
13 2014, note that something like 11 percent of all Internet
14 users use Tor for at least some of their browsing.

15 A. I'm not familiar with the specific report you're citing.

16 Q. Are you familiar with the general usership, at what
17 percentage people generally use Tor, how many people use it?

18 A. My investigations solely focus on people who use Tor for
19 illegal purposes, so I can tell you about those numbers. I
20 don't generally collect or research other users of Tor. It's
21 not relevant to my work.

22 Q. You're not really qualified to talk about what legal uses
23 exist for Tor or how popular it is outside of the context --
24 your experience with Tor is limited, really, to illegal uses
25 of Tor.

—D. Alfin - Redirect—

1 A. I can answer multiple questions about the Tor network, I
2 just can't affirm the number that you quoted earlier because
3 I'm not familiar with that specific study.

4 Q. We talked about how you can't find Tor-hosted sites
5 through traditional Internet searches like on Google or Bing,
6 right?

7 A. That is generally true, yes.

8 Q. There are search engines that work on the Tor network,
9 correct.

10 A. Not in the same context that they work on the regular
11 Internet. There are index Web sites of Tor hidden services
12 that can be searched, but their functionality is different
13 from, say, Google or Bing. But there are searchable index
14 Web sites that you can use to find addresses to Tor hidden
15 services.

16 Q. And I believe we talked a little while on direct about
17 someone's ability to stumble upon the Playpen site, right?

18 A. Yes. It would be very unlikely for someone to innocently
19 log in to Playpen without previously knowing what its content
20 was.

21 Q. Okay. Well, a number of the entries in the Playpen table
22 of contents could relate to adult pornography as easily as
23 they could to child pornography. Is that fair to say?

24 A. No. Playpen was dedicated entirely to child pornography.
25 All the topics on Playpen related to child pornography.

—D. Alfin - Redirect—

1 Q. And you're familiar with terms that are associated with
2 child pornography as part of your training, right?

3 A. I am.

4 Q. You're also familiar with terms that are associated or
5 can be associated with legal pornography, correct?

6 A. I am.

7 Q. Because it's important for you to be able to distinguish
8 between terms that may be specifically signalling child
9 pornography versus those that are possibly including adult
10 pornography or legal pornography, right?

11 A. That's fair to say.

12 Q. So the term "kinky fetish" can refer to adult
13 pornography, correct?

14 A. It can.

15 Q. And that's a term that appeared on the Playpen table of
16 contents.

17 A. And in the context of the Playpen Web site it is related
18 to child pornography.

19 Q. My question is asking whether the term that appeared on
20 the table of contents -- right? -- can be associated with
21 adult legal pornography.

22 A. Within the context of the table of contents, no, because
23 Playpen was a child pornography Web site. Outside of the
24 context of the Playpen Web site, yes, it can.

25 Q. Okay. So the answer to my question is that the term

1 "kinky fetish," in and of itself, can refer to legal adult
2 pornography.

3 A. That is a different question, and the answer to that
4 question is yes.

5 Q. Okay. The same question that I just asked you with
6 respect to bondage. That term, in and of itself, can refer
7 to legal adult pornography.

8 THE COURT: Well, there's no sense going through all
9 that, Counsel. I get your point.

10 MR. GRINDROD: Thank you, Your Honor.

11 BY MR. GRINDROD:

12 Q. And, so, with respect to stumbling upon the Web site --

13 MR. GRINDROD: Well, I'll leave it at that, Your
14 Honor.

15 BY MR. GRINDROD:

16 Q. Let me ask you one question about the NIT and the way the
17 IP address is sent back to the FBI.

18 I believe on cross-examination you testified that the
19 NIT gathered certain information from the activating
20 computer, like the host name and MAC, some of that
21 information we talked about, and then sent it back to the
22 FBI, correct?

23 A. That is correct.

24 Q. And then the FBI looked at that transmission, and it got
25 the IP address from the transmission.

—D. Alfin - Redirect—

1 A. That is correct.

2 Q. Now, the NIT was downloaded without the user's knowledge
3 or consent, correct?

4 A. They downloaded it without their knowledge, that is
5 correct.

6 Q. Okay. And without the NIT no user, including Mr. Matish,
7 would have been sending their host name or any other
8 information from their personal computer to the FBI, right?

9 A. That is correct.

10 Q. And so without the NIT the government doesn't get the IP
11 address, right?

12 A. That is correct.

13 MR. GRINDROD: I have no further questions, Your
14 Honor.

15 MS. GRATTON: Nothing further, Your Honor.

16 THE COURT: You may step down.

17 THE WITNESS: Thank you, Your Honor.

18 *****

19

20

21

22

23

24

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

CERTIFICATION

I certify that the foregoing is a correct transcript
of an excerpt from the record of proceedings in the
above-entitled matter.

/s

Heidi L. Jeffreys

May 20, 2016

Date