CROSS-EXAMINATION

MR. DRATEL

Q. Good morning, Mr. Miller.

A. Good morning.

Q. You just testified on direct about that March 16th post at 3:39, I think it's Exhibit 1200.

A. Yes.

Q. Right?

A. Yes.

Q. I want to go back about 20 minutes earlier in the timeline and ask you a few questions about the process of logging on in which you -- this user account logged onto the Stack Overflow.

A. Okay.

Page 1349
Q. So, Stack Overflow accepted a method of logging on called OpenID, is that correct?

A. That's correct.

Q. And OpenID is a system that essentially allows people to log in to multiple websites without having to enter the username and the password for each website, right?

A. Correct.

Q. And it works by establishing -- and establishing the person operating a web browser is who they claim to be, right?

A. Yes.

Q. And we're talking about any web browser, whether it be Internet Explorer, Mozilla, Firefox, Google, right?

A. Yes.

Q. Now, as vice-president of operations, right --

A. Correct.

Q. -- at Stack Exchange --

A. Yes.

Q. -- you're aware that there are security flaws with the OpenID system, correct?

A. I'm not familiar with the technical details of them.

Q. Are you familiar with literature with respect to security researches from Microsoft and computer scientists from the University of Indiana at Bloomington about OpenID?

MR. TURNER

Objection; foundation, hearsay.

THE COURT

If the answer is "no," then it's straightforward. We'll take it one question at a time. I'll allow this.

A. I am not, at least not having actually read it.

Q. Are you familiar with a term called covert redirect?

A. Yes.

Q. And that's when someone steals personal data from a user, right?

A. Yes.

Q. And OpenID is something that can be vulnerable to covert redirect, right?

A. My understanding is that it could.

Q. Also you said that all you really need to register is an email address and a username, right?

A. Correct.

Q. So if I had your email, I could register as you and just put a different username, right, with your email?

A. Yes.

Q. So all I have to do is know an email address for someone else to sign onto Stack Overflow, use that email address with whatever username I chose, right?

A. Yes.

Q. And there's no way from the records that we've seen or the records that you have to determine who the actual person is who is using that email account to register, correct?

A. No. We -- if I'm understanding your question correctly, all we do is basically look at the email account. We don't try and look into who the actual person is.

Page 1351
Q. Right. So you wouldn't know from your records who is using that email account to register on Stack Exchange or Stack Overflow?

A. Correct.

Q. And there's nothing in your records that would help us determine whether or not the use of the OpenID system to get into that account was the subject of some covert redirect attack, right?

A. Correct.

Q. Now, just looking at the sequence of events that you testified to earlier, so the first thing that the person who registered did was use the email rossulbricht@gmail.com, right?

A. The account was originally created using Facebook Connect, so the email address would have been passed automatically by Facebook as part of that authentication.

Q. But that's the email that was on the account?

A. That's the email that Facebook tells us who is on the account and, therefore, the email that we added to the account.

THE COURT

What is Facebook Connect?

THE WITNESS

It's a service that allows a website such as ours to allow someone to use a Facebook account to establish their account on our website.

THE COURT

All right.

Page 1352
THE WITNESS

It's their version of the OpenID.

Q. So it's a version of OpenID essentially?

A. Yes.

Q. And subject to the same vulnerabilities that we just talked about with respect to OpenID?

A. I'm not familiar with the technical implementation details on it, but in theory, yeah, I would suppose.

Q. And then 30 seconds later, the username changes to frosty, correct?

A. No. The username frosty wasn't changed until the following year.

Q. Following year?

A. Sorry. Can you repeat the question?

Q. Yes. On March 16, 2013, at 3:39:25 a.m. the user posted a question "How can I connect to a Tor hidden service using curl and php," correct?

A. Yes.

Q. And put specific lines of code in the message, correct?

A. Yes.

Q. And available essentially for the world to see, correct?

A. Correct.

Q. And you keep all of those records, right?

A. Yes. We make them --

Q. And even if someone changes their screen name or their username, you would still have all the original records, right?

A. Yes.

Q. And they would be available by subpoena, right?

A. Yes.

Q. But we have that first entry, March 16, and that's Exhibit 1200, right, 3:39:25 a.m.?

A. Yes.

Q. And that's UTC time, by the way?

A. That's correct.

Q. So, at approximately 30 seconds later March 16, 2013, the user changes the screen name to frosty, right?

A. Yes.

Q. So thereby establishing without any question for anyone subpoenaing those records that frosty and Ross Ulbricht are connected, right?

MR. TURNER

Objection, form.

THE COURT

Sustained.

Q. So it doesn't change the fact that you still have all the original records available by subpoena, right?

A. Correct.

Q. Kind of a blinking neon arrow, isn't it?

MR. TURNER

Objection.

THE COURT

Sustained.

MR. DRATEL

Nothing further, your Honor. Thank you.

THE COURT

Redirect?

MR. TURNER

Very briefly.

THE COURT

All right.

REDIRECT EXAMINATION

MR. TURNER

Q. You said when the account was originally registered, it was registered using a Facebook account?

A. Yes.

Q. Would the user of that Facebook account had to have been logged into his Facebook account in order to register with Stack Overflow in that manner?

A. Yes.

MR. DRATEL

Objection; foundation.

THE COURT

Overruled.

Q. And just to make sure the timeline is clear, the account was registered in March 2012, right?

A. Correct.

Q. And from 2012 until March 2013, the display name for this user was Ross Ulbricht, correct?

A. Correct.

Q. And the registered email address was rossulbricht@gmail.com, right?

A. Correct.

Q. Not until the post we saw in 2013 did that information change, right?

A. Correct.

MR. TURNER

No further questions.

Page 1355
MR. DRATEL

Just a couple, your Honor.

RECROSS EXAMINATION

MR. DRATEL

Q. Now, you don't know how the person logged in, though, to make that post, correct?

A. In -- sorry. In which case?

Q. In 2013? In other words, to log into Stack Overflow in 2013, they used the OpenID system?

A. Correct. They used the OpenID through Google.

Q. Right. So it didn't necessarily have to come through a Facebook account?

A. No. In this case, if I'm understanding your question correctly, we key -- we do what's called keying on the email address. So any OpenID-type system that you use if it returns the same email address because that trusted third party trusts -- says that that is the email address of this person, we trust that it is the email address of the user at the time.

Q. Right. So in March of 2013 when that post was made, I could have typed in "rossulbricht@gmail.com" and had the right -- and that would be it, right? I would be in there?

A. Google would have to tell us that the person on the computer -- if you were to do that, we would be trusting Google to tell us that you had control over that Gmail address at that time.

Q. But that's what essentially the OpenID system does, right?

Page 1356
A. Yes.

Q. With respect to the register of an account that you say is on Facebook, but obviously you don't know who is on the Facebook account when they're registering, right?

A. Correct, correct.

MR. DRATEL

Can I have one moment, your Honor.

THE COURT

Yes.

MR. DRATEL

Nothing further. Thank you.

CROSS-EXAMINATION

Page 1241
MR. DRATEL

Q. Good morning, Mr. Beeson.

A. Good morning.

Q. I just want to go back to something I showed you last week Thursday and show you a different version. This will be Defendant's H and ask if you recognize that.

A. I do recognize it as one of the pictures I took.

Q. Of the laptop while you were working with it?

A. Yes, this is a screen shot.

MR. DRATEL

OK. I move it into evidence, your Honor.

MR. TURNER

I have no objection.

THE COURT

Received; Defendant's Exhibit H.

MR. DRATEL

Thank you.

MR. TURNER

So looking at "H" we can get it published.

(Pause)

Q. And looking at "H" you see on the top of that line across and that's a bitcoin client program operating right where it says the Colbert report?

A. Unfortunately, I don't know for sure what it is. I can see that it says the Colbert report but I don't know what kind of application it is.

Q. But if you look at the metadata that's part of this exhibit now which -- did that enable you to recognize it, by the way?

A. Yes, it did. Thank you.

Page 1242
Q. So that's the 7:56 p.m. on October 1, 2013?

A. That's what it says, yes.

Q. 40 minutes off?

A. 40 minutes off.

Q. Which way though?

A. It's slow. So we'd have to add 40 minutes to this time making it 8:36.

Q. 8:36 p.m. San Francisco time?

A. Yes, sir.

Q. And it says 197 -- no, it says 197 megabites uploaded 26.10 MB, right? Do you see on top of the red line?

A. Yes, I do.

Q. Now, you took these photos after you had already imaged the laptop, correct?

A. My recollection is that the laptop was in the process of being imaged. In other words, I had started the process and was taking these photographs at that time.

Q. Did you testify Friday that you had already made your copies that you took the photos after you had imaged it?

A. I would have to refer to my notes to be sure on the times. A lot of times things are done as I go. You know, once I start something I can start something else. So exact times I can't recall.

MR. DRATEL

I just want to publish for a second Defendant's G which is already in evidence.

Page 1243
(Pause)

Q. And there it says "uploaded 8.35 megabites". Can you see that?

A. It's a little blurry on my screen but it looks like it could be 8.35.

Q. OK. An on the one that we just saw that you took it's 26.1 megabites, right?

A. Yes.

Q. So, are you not familiar with the program that's running on Defendant's H?

MR. TURNER

Objection; asked and answered, beyond the scope and relevance.

THE COURT

Sustained.

Q. And you didn't generate the MD5 hash value for the laptop until October 3 when you started the RAM capture?

A. Correct.

Q. And the RAM capture is essentially the running memory on the laptop?

A. Yes. RAM is random access memory, that's correct.

Q. Can you just define that for the jury, please?

A. Yeah. So, random access memory is the memory in your laptop or computer that's used by not hard drive storage. It is that instantaneous memory that the basic code for the programs get loaded into RAM and then your computer can use it in there.

Page 1244
Q. And that gives you a window -- it gives you a ability to see what processes are running on a computer, right, RAM?

A. Whether it gives you what processes are running -- everything get's loaded into RAM. So all the binary codes, all the codes that the computer needs to run is loaded into RAM. That could be the active process. That could be the operating system and so forth.

Q. So on October 3 which is two days after you received the laptop you began to do the RAM memory capture?

A. That's correct. One of my associates and I just to be clear.

Q. And you weren't quite sure how to do that RAM capture, correct?

A. The RAM capture was nontrivial.

Q. Right. But you weren't quite sure how to do it. You asked for assistance, in fact?

A. I did.

Q. You asked whether there was a RAM capture tool that you could use for it?

A. That's correct.

Q. And this is a relatively new field in computer forensics, RAM capture?

A. No. I wouldn't say it's a new field.

Q. Well, one of the things that is part of the RAM capture is encryption keys and passwords and other things that are stored in the memory, right?

Page 1245
A. That's correct.

MR. TURNER

Objection.

THE COURT

Overruled.

Q. And the processes that the computer -- the process of the computer programs that are running on the computer is something else that RAM can tell you, RAM memory capture would be able to reserve for you?

A. That information can be in RAM.

Q. And the active network connections at the time that the capture occurred would be something else?

A. It can be. It doesn't necessarily mean that it is.

Q. And it could also determine whether there were malware or viruses or other programs running on the system, correct?

A. It could be, yes.

Q. Now, you've used a piece of software called FMEM, F-M-E-M, to try to acquire the RAM memory?

A. That's correct.

Q. And system memory is broken down into registers called ranges; s is that right?

A. That's correct.

Q. And for FMEM you have to specifically point the program at the registers that you want the system that you'd rather that you want to capture, right?

A. That's correct. The RAM is divided into chunks, into groups, so to speak. Some are more protected
Page 1246

Q. OK. And so -- and if you don't direct the capture process at the right registers of RAM they will go to something called uncachable, U-N-C-A-C-H-A-B-L-E?

A. I believe so.

Q. And you weren't sure at the time about this, is that fair to say?

A. Well, this is why I obtained the help from one of my associates.

Q. But in fact, the FMEM capture did not work entirely, correct?

A. Upon capturing what I believe was the third register or third section of the memory FMEM crashed the computer.

Q. And when it crashed the computer you were no longer able to get any of the RAM capture that you had not gotten initially, correct?

A. We were able to continue with the capture after the computer was restarted.

Q. Now, you in doing your RAM capture you consulted the manuals on the computer in an attempt to find out how to proceed, right?

A. I don't recall consulting any manuals on the computer.

Q. Did you keep a running roster of commands that you issued the computer during your work?

A. Yes, we did.

Page 1247
Q. I am going to show you what's marked Defendant's I for identification -- "K", I am sorry. Call it Defendant's K for identification. And ask you to look at page two of this document. I ask you if that refreshes your recollection that you consulted the manuals on the computer?

A. These are not the manuals for the computer. These are manuals for the applications MEMDUM and FMEM that may or may not have been on the computer.

Q. Right, but you were looking for them?

A. Yes.

Q. And did you find one for MEMDUM?

A. I don't recall whether one came up or not.

Q. Well, there's no such file for that on a Lenox system, is there?

A. There could be. Depends on the Lenox system. Most likely there was not but I don't remember for certain. Chances are since I then checked for a manual for tool FMEM that there was no tool for MEMDUM on the system.

Q. And so you never got a full RAM memory capture, correct?

A. Can you define a full RAM memory capture, please?

Q. Well, why don't you.

A. Well, the difficulty in RAM capture is that it's live, so it's ever changing and it's ever active. When we captured what I believed was the third register or third group of memory from the RAM, the system crashed which is not that uncommon in RAM captures. And so after we were able to restart we restarted with our own version and move onto the next and we continued to capture the other registers that were still there.

Page 1248
Q. But when you had the capture open before it crashed it has all the operations going, correct?

A. Yes.

Q. And so once it crashes and then you reboot it, you've lost all of that information that's included that went live before it crashed, right?

A. You do not lose all of the information.

Q. But you lose information?

A. Do you lose information.

Q. And you don't know what information you lost?

A. You do not know.

Q. And that information is lost to us forever, essentially?

A. It is.

MR. DRATEL

Nothing further, your Honor.

THE COURT

All right. Thank you.

Mr. Turner, anything further from the government?

MR. TURNER

One moment, your Honor.

(Pause)

MR. TURNER

Briefly, your Honor.

REDIRECT EXAMINATION

MR. TURNER

Q. Agent Beeson, I talked to you about how when you are doing a live capture, things are changing. Could you explain a little bit more what that means if you type something on a keyboard just a single press of a keyboard does that change --

Page 1249
A. Yeah. So in performing a live capture of basically capturing data from a running computer whether it be from the hard drive or from the RAM, everything that we do is to some degree altering information. And so our goal is to minimize that alteration to the maximum we can but we do have to use the computer in order to capture this information.

Q. So the sort of alterations you are talking about thought, does that involve --

A. Absolutely, not. It's very minimal footprint. We were trying our very best to not alter anything to the extent we can.

Q. You talked about some errors you ran into or crashes. Any of those prevent you from making a full and complete copy of the Lenox half of the computer that we talked about on direct?

A. No, it isn't.

Q. And those errors, could any of those errors have resulted in the generation of thousands of pages of TOR check logs on the computer that weren't there before?

A. Absolutely, not.

MR. TURNER

No further questions.

MR. DRATEL

Briefly, your Honor.

THE COURT

All right.

Page 1250
RECROSS EXAMINATION

MR. DRATEL

Q. But the RAM capture, we lost the ability to see what the computer was doing at that time, correct, in the full range of it, correct?

A. Yes.

Q. Including connections to the internet, correct, in connection with what was going on with the internet?

A. I supposed. That's define as anything it's part of the group of things that could be in there.

Q. And the questions of malware and viruses and whatever else might have been on there we'll also never know, right?

A. Potentially.

MR. DRATEL

Nothing further. Thank you.

THE COURT

All right. Thank you.

MR. TURNER

Excuse me. One more question, your Honor.

THE COURT

One.

REDIRECT EXAMINATION

MR. TURNER

Q. The RAM capture didn't prevent from you seeing what historically had been on the computer from years before?

A. No.

MR. DRATEL

Objection as to form.

THE COURT

Overruled.

Page 1251
RECROSS EXAMINATION

MR. DRATEL

Q. You have no idea when anything was put on that computer, right?

A. I did not conduct the forensic exam on that computer, so.

THE COURT

All right. Thank you. You may step down, sir.

MR. TURNER: No further questions.

THE COURT: Mr. Dratel.

MR. DRATEL: Thank you, your Honor.

CROSS-EXAMINATION

BY MR. DRATEL:

Q. You just mentioned that you took some photographs of the laptop?

A. Yes, sir, I did.

Q. And the ones that you put in evidence were not the only photographs, correct? You took additional photographs?

A. That's correct.

Q. Let me show you what's marked as Defendant's H --

A. Thank you.

Q. -- and just ask you if you recognize that.

A. I can't say that I do recognize this as one of the photos I took. I may have. I took numerous photos of open screenshots. I would have to see the file information or the metadata relating to this photo to confirm it.

Q. Okay. I'll go --

A. Because I did take several shots.

Q. Yeah. And several shots of the laptop, right?

A. That's correct.

Q. I'll move on. We'll find them. So, in terms of trying to capture what was on the laptop, the use of the tar command, correct, T-A-R?

A. That's right.
Q. That's to archive the files that you tell it to copy, right?
A. That's correct.
Q. The command is really just essentially like any other command on a computer, just telling the computer what to do with a keystroke or series of keystrokes, right?
A. Yes, sir.
Q. Essentially, it reads those files and then places them in an archive, the tar command, right?
A. That's correct, much like a zip file, sir.
Q. And but by doing this, you change all the access times for all those files that you're tar'ing to the time when you tar, right?
A. The access times can be changed; yes.
Q. Isn't that what happened here, that the access times were all changed by that tar'ing command?
A. Because I'm not the forensic analyst on this case, I don't know exactly whether or not those were changed.
Q. Well, there's a way to tar without changing access dates, right?
A. I am not familiar with the way for sure.
Q. But if the access files are changed, then they only reflect the time that you tar'ed it, right, and not the access files that existed on the laptop itself?

A. If, in fact, the access times were changed as part of the archiving process, then, yes, they would have been changed to the current time when the archive was created.
Q. Now, you're familiar with the Guidelines for Evidence Collection and Archiving issued in 2002?
A. Not specifically, sir.
Q. Are you familiar with a section that says don't run programs that modify the access times of all files on the system, e.g., tar or X copy?
A. If I'm not familiar with the section, I wouldn't be familiar with that specific --
Q. Now, while you were running the tar command on the Frosty directory -- and by the way, Frosty is the main directory on the computer?
A. It's the home directory.
Q. The home directory.
So you received an error message, correct?
A. While I'm tar'ing?
Q. Yes.
A. I may have.
Q. Do you recall?
A. I don't recall for certain.
Q. Let me show you what's part of 3512-1. 3512-1 -- and I'll give you the entirety of it so that you can look at it. Just ask you to look at page three, this is double-sided, and that

second paragraph.
A. Sure. May I ask you for clarification. I just want to make sure I'm at the right photograph. It starts "Frosty user folder"?
Q. Yes.
A. I'm ready.
Q. Does that refresh your recollection that you received an error message during the tar process?
A. Yes, it does. These are my notes.
Q. Yes. I'm saying that refreshes your recollection. I have to ask a question a certain way for evidentiary purposes.
A. Yes, it does, sir.
Q. Okay. Thank you.
And the error message was "File changed as we read it exiting with failure status due to previous errors." Right?
A. That's correct.
Q. And at that point, you weren't sure whether you had properly copied all of the files -- whether the tar process had been completed at the point that you got that error message, correct?
A. That's correct.
Q. And there are a number of possible reasons for that kind of error message, right?
A. Yes.
Q. And one is that while the -- as you mentioned -- withdrawn.

Just go back a bit. You talked about live capture versus the machine being off, correct?
A. Yes.
Q. So if the device is off, then you're not worried about changing files, right, but while it's on, files can be changing while you're tar'ing, right?
A. That's correct. It's a live file system, so things are happening constantly.
Q. Right. And that's one of the possible reasons for an error message, correct?
A. It's a likely explanation for this error message.
Q. You didn't know precisely, though, right, and you don't know even today what the precise reason for that error message was?
A. I don't, nor do I know the file that caused the message.
Q. And when you created the disk image of Mr. Ulbricht's laptop, you didn't use any proprietary computer forensic software, right?
A. I did not.
Q. And that's -- some of that software can automate the process of capturing a hard drive image?
A. In a live capture scenario, sir?
Q. Well, is that different?
A. It is.
Q. All right. So you used a piece of software called DD,

right?
A. Yes.
Q. And that's built into many Linux-based operating systems?
A. Yes.
Q. And that's a delicate program, right?
A. It's a powerful program.
Q. In the computer world, doesn't DD have a widely-accepted meaning in the forensics community for disk destroyer?
A. I'm not familiar with that. I've -- I've heard it or read it, but it's not what it means.
Q. But it can have disastrous consequences for imaging if a mistake is made, correct?
A. Yes. As I said, it's a powerful tool.
Q. And so at 7:42 p.m. that evening, the first of October, you attempted to generate an MD5 Hash value of the device mapper of on the drive on the computer, right?
A. Of the folder depth mapper.
Q. What did you attempt to get an MD5 Hash for?
A. Well, I attempted several MD5s, so I just want to make sure I'm answering.
Q. At 7:42.
A. One moment. Okay. Could you repeat that question for me, sir.
Q. Sure. Yes. At 7:42 p.m., 1942 hours essentially, you attempted to get -- to generate an MD5 Hash value, right?

A. Actually, what I was attempting to do was to DD the disk, to make a copy or an image of the disk; and at the same time, take that data stream as I read it and pipe it into MD5 sum which would generate my digital fingerprint of the disk at the same time.
Q. Right. And that failed, right?
A. It did.
Q. Permission was denied?
A. That's correct.
Q. So, then you re-performed the command, though, but without doing an MD5 Hash value at the same time, correct?
A. That's correct.
THE COURT: You have just a couple of minutes left on today's session, Mr. Dratel.
MR. DRATEL: I don't know that I'll finish, your Honor.
THE COURT: Just to let you know that we'll end at 5:00.
MR. DRATEL: Okay. Thank you.
Q. Now, the live capture environment, because you're not sure what -- you're not capturing an inactive image, that the image is active, it's called slurring; is that right?
A. I'm not familiar with the term slurring.
Q. Well, you knew that the DD file that you created was not a replica in exact terms of computer forensic terms of the hard

drive because of the active file system at the time, right?
A. It was a replica at the instantaneous point in time when it was made.
Q. But it wouldn't match the DD file you created even a second later?
A. It would never match because every time I typed something into the keyboard, parts of the file system would change again.
Q. And you didn't generate the MD5 Hash until a couple days later, correct, October 3?
A. That's correct.
Q. And that was when you had started the random access memory - what we call RAM - capture of the laptop, correct?
A. That's correct.
Q. And are you familiar with the term "order of volatility" in terms of computer forensics?
A. I am.
Q. So you attempt to capture the most volatile parts of the system first, which is the memory, correct?
A. I think in this instance it's arguable.
Q. But that's the general principle, right?
A. The general principle is, yes.
Q. But you didn't try to capture the memory until you'd already done two other processes, correct?
A. That order was very carefully selected; yes.
MR. DRATEL: I'm kind of going into a different area,

Judge.

THE COURT: How much more do you have?

MR. DRATEL: I probably have about ten to 12 minutes left.

THE COURT: Ladies and gentlemen, we will break for today and come back on Monday. And I want to remind you not to talk to each other or anybody else about this case. I also want you to make sure that if you run into any media or news articles about this case, that you avert your eyes and that you don't update your Facebook account or do any tweeting about this case of any kind.

We'll pick up on Monday at 9:30, and I'll see you then. Thanks very much. Have a good weekend.

(Jury excused)

(Continued on next page)

And that's a paragraph of the Glen Park library, correct?
A. That's correct, yes.
Q. And that's where Mr. Ulbricht was arrested, right?
A. Yes.
Q. He was arrested -- if we can enlarge the right part, I guess, yes. That's fine. He was arrested at the table where the person is sitting against the window, is that right?
A. Yes.
Q. And in fact, Mr. Ulbricht was sitting not where that person is, but he was actually sitting with his back to where we are and he was looking out the window, right?
A. He was -- what I remember, he was just like that.
Q. You've been interviewed in preparation for your testimony, correct?
A. Yes.
Q. You sat down with the government, right?
A. Yes.
Q. More than once, right?
A. Several times.
Q. Yes. And didn't you tell the government that Mr. Ulbricht had his wack to you looking out a window? Didn't you say that twice to the government?
A. I don't -- do you have anything to show me?
Q. Sure. I'll show you what's marked as 3508-2 and 3508-7. If you could look at 3508-2 and 3508-7 and the first

highlighted portion on that page and the highlighted portion on that page.

A. Sure.

Q. Does that refresh your recollection, that you told the government twice in preparation for this case that Mr. Ulbricht's back was to you and he was looking out the window?

A. I don't know what these are, but that's what it says there, yes.

Q. And could we go to Government's Exhibit 225B, please. If we can scroll down a little bit. This is a conversation that you -- you didn't read it. Mr. Howard read it yesterday, right? This is something you got off the laptop, right --

A. Correct, yes.

Q. -- you got off the drive that was given to you? The highlight version reads -- and this is -- just to put this back in context, this is Dread Pirate Roberts and this is on a TorChat, right?

A. These are from the TorChats, yes.

Q. And Dread Pirate Roberts is responding to someone working for him that the person is concerned about being arrested, right, about law enforcement?

And Dread Pirate Roberts responds "There is nothing on your laptop for them to use, if you obscure your bitcoins properly, there's there is no way for them to trace them back

to me. Realistically, the only way for them to prove anything would be for them to watch you log in and do your work," right?

That's Dread Pirate Roberts, right?

A. That's what it says.

Q. And that's January of 2013, right?

A. Yes.

Q. So if we could go further. Again Dread Pirate Roberts: "Sure, someone could stand behind you without you realizing it," right? Yes?

A. Yes.

Q. So Dread Pirate Roberts understood full well the dangers of having his back to anyone who could sneak up behind him, right?

MR. HOWARD: Objection; speculation.

THE COURT: Sustained.

Q. You testified yesterday, right, that the argument dispute that was contrived to distract Mr. Ulbricht was, in fact, behind him, right, and he turned around?

A. Yes.

Q. So if we go back to 228 -- I'm sorry -- 128H, Mr. Ulbricht really couldn't be sitting in that spot where that person was against the window because the other two people would have to be behind him, right?

A. That's where I remember him.

Q. But you told the government twice in preparation for this case that he had his back to you looking out the window?

A. It's here. It's in this document here.

Q. You deny that you said that?

A. Yeah, I mean. I don't deny I said it, but it's here in the document. If that's what that is, then, yes, I said that.

(Continued on next page)

Q. OK. Now, just going back to 228 -- I'm sorry, 225B, which we were just looking at.

So if we go back up a little further to the first part, so it says: "There is nothing on your laptop for them to use. If you obscure your bitcoins properly there is no way for them to trace them back to me."

But all of the material that you put in yesterday, and some of what you put in today, came from an image that Mr. Beeson provided to you from Mr. Ulbricht's laptop?

A. That is correct.

Q. The journals, right?

A. Yes.

Q. The Tor chat logs; thousands of pages of Tor chat logs, right?

A. Yes.

Q. PGP keys, right?

A. Yes.

Q. Now, you have a background in security, correct, in Internet security, right?

A. Yes.

Q. You have taken courses; you have trained that way, right?

A. Yes.

Q. And aren't you -- isn't it part of the security for a PGP key is not to make it available on your computer, your private key?

MR. HOWARD: Objection to form.

THE COURT: Sustained. You can rephrase.

BY MR. DRATEL:

Q. Isn't it a fundamental part of security not to keep your PG -- your private PGP key available on your computer in a manner that can be viewed by anyone on that computer?

A. No. You have to -- the key has to be somewhere. If you set it up on your computer, that's where you would keep your key. The idea behind it is to store it in a safe location, like an encrypted, again.

Q. And you put it in a file that says "Key," is that a good way to disguise it?

MR. HOWARD: Objection.

THE COURT: Sustained.

Q. But you wouldn't put it in a file -- would you as a person trying to be secure put it in a file with the name "Key" on it?

MR. HOWARD: Objection.

THE COURT: Sustained.

Q. Do you instruct people on how to disguise PGP keys on their computer?

A. I don't --

Q. Have you been instructed? Is there training on that?

A. Is there training on that? No, there is no training on where to keep your PGP key. It is your secret key. So if I was doing it, I would have an encrypted laptop and keep my key

there, and when I turned off my laptop the key would be safe.
Q. And you would put it in a file called "key"?
MR. HOWARD: Objection.
THE COURT: Sustained.
Q. And when you say -- throughout your testimony, you said "pulled off the defendant's laptop," "pulled off the defendant's laptop." In fact, what you're working with is not the defendant's laptop, correct?
A. Not the -- it's a copy of what was on the defendant's laptop.
Q. Right. It was a copy that you didn't make?
A. A copy I didn't make, no.
Q. Right.
A. That is correct.
Q. It is what you received from Mr. Beeson?
A. Yes.
Q. So when you say "off the laptop," "off the laptop," it is really off of a copy of a copy, right? In other words, Mr. Beeson gave you a hard drive that was not the hard drive from the laptop but an image of the laptop?
A. That is correct.
Q. And then you made a copy of that and worked off of that?
A. Yes.
Q. So -- and you didn't participate in the imaging that Mr. Beeson did, correct?

A. That's correct.
Q. Also, when you said -- sometimes you said it's up to the designers of the site, right, in terms of certain issues with respect to Web pages and things like that?
MR. HOWARD: Objection to form.
THE COURT: Overruled.
A. I did, yes.
Q. And when you -- and when you say "designers," that doesn't mean that it can't be modified at some point, right, by other people?
A. The names of it?
Q. The way the site appears, the names of fields and the way of the Web pages.
A. Sure, it could be changed, again, by the designer or --
Q. When you say "designer," it doesn't have to be the same designer as the initial designer, it could be other people later on, right?
A. Yes.
MR. DRATEL: Now, if we could go to Government's Exhibit 201A, please.
Go further up. Go to the metadata.
(Pause)
Q. So this is the one where your phone -- you are taking this with your BlackBerry, correct?
A. That is correct, yes.

Q. And your BlackBerry registers East Coast time, right?
A. It does, yes.
Q. Even though you're standing in the Glen Park library in California, your electronic device in your hand has East Coast time, right?
A. It does, yes.
Q. So it doesn't reflect where you are?
A. Time zone, no.
Q. Right?
A. Time zone, no. Physically I'm still in San Francisco.
Q. Right. So the time zone reflected in your electronic device in the metadata is not accurate as to where you actually are?
A. That's correct.
Q. So metadata is just digital data, right?
A. It is.
Q. Now, we talked just for a second -- you have training in network security, correct?
A. I do.
Q. And you were an informational technology -- information technology specialist, is that one of the positions you have held?
A. Yes.
Q. So could you explain what that involves in terms of training?

A. Information technology specialist?
Q. Yes.
A. Yes. That is more on the side of maintenance and things to that nature of computer systems.
Q. Keeping networks secure?
A. Keeping networks secure.
Q. Teaching best practices to people who work on networks?
A. Just, again, managing computer systems for users and things like that.
Q. Now, by the way, the photos that we've seen that you've put in evidence were not the only photos that you took of the laptop, correct?
A. No. No.
Q. I want to show you what's marked as Defendant's G, for identification.

I will give you the original.

A. OK.
Q. And I ask you if you recognize that?
A. I do.
Q. Is that a photo that you took?
A. It is, yes.
Q. Is it a photo of the defendant's laptop that you took October 1, 2013, at the time -- at or near the time of his arrest, or shortly after his arrest?
A. Yes, it is.

MR. DRATEL: I move it into evidence, your Honor.

THE COURT: Mr. Howard.

MR. HOWARD: No objection.

THE COURT: Received, Defendant's Exhibit G.

(Defendant's Exhibit G received in evidence)

MR. DRATEL: Thank you, your Honor.

So if we could publish it, please.

Q. Now, this window shows one of the programs that was operating at the time of Mr. Ulbricht's arrest, correct?

A. It does, yes.

Q. And it is a program called BitTorrent?

A. It's called TransMissions but it is a BitTorrent client, yes.

Q. Right, it is a BitTorrent client. Could you explain what that means?

A. It is a file sharing program that allows you to -- it allows you to upload and download files that you want to look at. It's based on seeds that are up on the network that you pull. You pull down the seed and you can populate your data with -- populate your folders with the data.

Q. And it is very popular for music and movies and things like that, correct?

A. It is, yes.

Q. It is called a peer-to-peer network, is that one of the ways this is described?

A. It runs on something like that, yes.
Q. And it involves your computer connected to the Internet, right?
A. Yes.
Q. I'm trying to break this down rather than have a compound question.
A. That's fine.
Q. Your computer connected to the Internet with all other people who are on that same network, that BitTorrent network, who are connected to the Internet, right?
A. Yes.
Q. In other words -- and they can -- if they identify files on your computer that they want to share, they can take them from your computer, right?
A. Not that easy but you have to give the Torrent to them to actually get files from your computer that you designate. It is not willy-nilly where you can go anywhere on your computer, but you designate spots that you can download from -- not put on but download from.
Q. But, in other words, you share the files, essentially?
A. Essentially you are sharing some of your files.
Q. And so this says, it says: "Sending to 7 of 9 connected peers," right?
A. Yes.
Q. So that means that there are seven computers out there in

the world that are actually connected to Mr. Ulbricht's computer right there?

A. To --

Q. Through this network?

A. To his specified location that he gave.

Q. Right. But to his computer?

A. Yeah, to his computer.

Q. Do you see what's downloading there is the Colbert Report, right?

A. Yes.

Q. It is not complete at that point, right?

A. It doesn't look to be.

Q. It only looks like about 8-and-a-quarter megabytes of 197 megabytes, right?

A. Yes.

Q. So that takes some time, correct?

A. Yeah. Depending on connection speeds and things like that, but yeah.

Q. So you have to have an open port to the Internet on your computer to operate BitTorrent, correct?

A. You do. The protocol is required that a port or a connection spot is open.

Q. And the fact that he's downloading at that time, that that process is going on, means that the port was open at that time, right?

A. It was connected.
Q. And that you know from your training makes one vulnerable, correct, to have an open port like that -- it makes your computer vulnerable?
A. That's how the Internet works. There is open ports on a lot of different surfaces. It is the nature of the Internet. Something has to get transferred back and forth. So, yes, a port was open on the machine to allow BitTorrent, that client, to work.
Q. But that also means that those with sophisticated computer skills could exploit an open port as well, correct?
A. Is it possible for that to happen? Yes.
Q. In fact, you could be exploited by hackers, by viruses, right; all sorts of things can get into your computer through BitTorrent? Even BitTorrent downloading, you can have viruses and malware that come with those files, right?
A. With the files you download?
Q. Yes.
A. Yes, they can contain programs that do things like that.
Q. I'm sorry. Programs?
A. There are programs that can be used maliciously, yes.
Q. Maliciously, including to operate a computer remotely, right, that kind of malware can be --
A. They make that stuff but it's again ...
Q. And knowing a port is open on a computer, for someone

trying to exploit that computer makes it easier to get in, right, if you know that there is a port there that's available?
A. That's incorrect. It is not easier. It gives you opportunities but it does not make it easier. It is the software guarding that port that is --
Q. But, I mean, it is easier than no port at all open, correct?
A. Yes. Again, that's how the Internet works. You have these ports that are open.
Q. And does the FBI allow you to run BitTorrent on your machine at work?
THE COURT: Let's have a sidebar.
(Continued on next page)

(At the sidebar)

THE COURT: I'm concerned that you're trying to make this witness into a general expert on BitTorrent. I have no problem -- obviously you are fully entitled to explore what acts this witness took with respect to the testimony he has given and explore his background in terms of whether he was qualified to do that. But you can't make him into a generalized expert on BitTorrent. This has gone far afield.

MR. DRATEL: That is my last question on this subject.

THE COURT: We are not going to this question. It is irrelevant with this witness. It's beyond the scope of his direct. All right? I mean --

MR. DRATEL: I don't think it is beyond the scope of his direct.

THE COURT: Absolutely. Are you aware that the FBI allows BitTorrent?

MR. DRATEL: It is for purposes of the security, in other words, the lack of security of BitTorrent.

THE COURT: That is not relevant. Whether the FBI allows BitTorrent on their computers is not relevant to whether or not the particular computer here -- you've got to establish that it was running BitTorrent. If you want to explore whether or not, if you've got a good faith basis to believe -- a good faith basis to believe that the files were placed on this computer, Mr. Ulbricht's computer, through the use of the

BitTorrent program, then go after that. But I am not going to let you go into the practices of the FBI.

MR. DRATEL: It is the practice -- it is a fundamental question of security. This is a completely insecure system for someone who --

THE COURT: That is not this case. Thank you.

Let's go back.

(Continued on next page)

(In open court)

BY MR. DRATEL:

Q. You have been trained and certified in the Linux operating system, correct?

A. Correct.

Q. A number of courses and certifications --

A. Yes.

Q. -- that you have taken with respect to Linux in particular?

A. Oh, yes.

Q. And you talked about the Tor chats that you created as a test, as an experiment, right?

A. Yes.

Q. And you saved them, right?

A. Yes.

Q. So could you describe the process by which you saved them?

A. Sure. Turn on the -- inside Tor chat in Tor chat client there is an enabling button that allows you to log your chats and save my chats.

Q. So, in other words, you had to affirmatively hit the enable button to save them?

A. Yes.

Q. So that was a decision -- conscious decision to save them on your part?

A. Yes.

Q. And Tor chats can easily be deleted from a computer, right?

A. Sure.
Q. You wouldn't even have to save them at all. Unless you hit the button, they wouldn't be saved?
A. Yes.
Q. And there are programs that can wipe away even any trace of what's happened on a computer previously, right?
A. Yes.
Q. And with respect to the chats that we saw, some of the ones -- and, again, Mr. Howard read them, you didn't read them, but some of them were snippets from chats, obviously, from a long series of chats, right?
A. That's right.
Q. And the snippets sometimes were different days and they were separated by a black line, right, some of them?
A. Yes.
Q. So those weren't all continuous; some of them were separated by time?
A. Yes.
Q. Now, that line that's on the top of each chat as it appears initially -- not in the way that it was done for purposes of reading them into evidence, but initially the line that says the log file is not signed and has no cogency of proof; do you recall that?
A. I do, yes.
Q. And that's automatically generated at the beginning of each

chat, right?
A. Yes.
Q. And that means that there is no way to validate that these particular log files were generated on that computer, correct?
MR. HOWARD: Objection.
THE COURT: I will allow it.
A. I'm sorry. Can you repeat that?
Q. Sure. What that means is that there is no way to validate that those log files were in fact generated on that computer?
A. Not generated but that's where they were saved.
Q. Right. OK. So it doesn't -- OK, not generated.
And those log files don't take up a lot of space, correct, about 15 kilobytes?
A. No, they're small. They are text files. They are not big. I don't know the size of them.
Q. And a kilobyte is about a thousandth of a megabyte, right, roughly?
A. Somewhere about there.
Q. 1024 bites to a megabyte?
THE COURT: Hold on. I think that because your question and his answer were interspersed, I'm not actually sure if it is 1024, which you want it to be, or a thousand, or if you care.
MR. DRATEL: I don't necessarily care. I was just trying to be precise.

A. 1024 is what it is, but we will go with a thousand.
Q. So those are files, because of the size of the files, the physical text files, they could be quickly transferred, correct?
A. Yes.
Q. Even over the Internet, correct?
A. Yes.
Q. And that is basically true for all the text files we saw, right, that they are small?
A. They are small --
Q. Ones -- even some of those spreadsheets are relatively compact, right, in terms of size?
A. Yes. It is not a huge file.
Q. And you talked about the mastermind screen.
A. Yes.
Q. And the mastermind.php file?
A. Yes.
Q. And the mastermind screen is the one that you found by hitting the back button, right, from the screen that was on the laptop when you first received it?
A. That's right.
Q. And did you have an opportunity to examine any of the other php files that were in that var/www directory?
A. Where? On the laptop?
Q. What you had, the copy that you had.

A. Yes.
Q. And do you know whether a user logging into the Silk Road site, using the password and username for the Dread Pirate Roberts' account, would automatically be directed to that mastermind page? Would that be -- do you know whether that would be the first thing that would come up?
MR. HOWARD: Objection. Beyond the scope.
THE COURT: Hold on. Let me just read his question.
(Pause)
THE COURT: I will allow it.
A. Can you repeat that?
Q. Sure. Do you know whether a user logging on to the Silk Road site, using the Dread Pirate Roberts' username and password to get on to the Silk Road site, would automatically be directed to the mastermind page?
A. I don't know.
Q. I am going to show you what's marked as Defendant's J and ask you to look at just first what it is. Do you recognize that?
A. Yes. The code looks familiar.
Q. Is that from the php files?
A. Yes.
Q. From the image that you were given of the laptop, right?
A. I don't know if from the laptop or the server.
MR. HOWARD: Objection to foundation.

THE COURT: Well, why don't you try to build a more concrete foundation.

MR. DRATEL: Sure.

Q. You've reviewed this document in the course of your investigation, correct?

A. Yes.

Q. That looks familiar to you?

A. This looks familiar, yes.

Q. And you don't know whether it is from the server or from the laptop, or could it be from both?

A. It could be from both.

Q. And it would be either from the Silk Road server or from the laptop image that you -- of Mr. Ulbricht's laptop that you reviewed, right?

A. Yes.

MR. HOWARD: Objection. Beyond the scope.

THE COURT: Well, I don't know whether it is or not. I have to see where this is going. I will allow a few more questions.

MR. DRATEL: OK. Thank you, your Honor.

I would move it in evidence, your Honor.

MR. HOWARD: Objection.

THE COURT: Well, I think that I'm going to receive it subject to connection. Obviously, whether it is in the server or the laptop, if that becomes important, then you will need to

determine which it came from. If that is an irrelevancy, then since it came from one or the other, there would be a sufficient foundation. So I would receive it.

So it will be received subject to any later testimony which may require a different ruling.

You may proceed.

MR. DRATEL: Thank you, your Honor.

THE COURT: Defense Exhibit J received.

(Defendant's Exhibit J received in evidence)

BY MR. DRATEL:

Q. So if you look at the lines that are marked on page 2, do you see that?

A. Yes.

Q. So from looking at those, is it possible now to answer the question as to whether a person logging on to the Silk Road site with the username and password of Dread Pirate Roberts would automatically be directed to the mastermind page?

A. I don't know.

Q. And, by the way, php -- I'm sorry, go ahead.

A. Like you said, I could read the php script and I could tell. I don't know.

Q. I'm sorry. You said you could read the php script?

A. I don't know the context of the script, that is all.

Q. Php is a script, essentially. We talked yesterday about operating systems, right, and so an operating system would be

Ubuntu as part of a Linux-based operating system, right, kind of like Windows --

A. Yes.

Q. -- or Mac; Yosemite I think is the current version. But php is what's called a scripting program, right?

A. It is, yes.

Q. And by that we mean sort of how you build a site, essentially, a website?

A. Yes.

Q. And is it somewhat similar to, in a Windows-based environment, say html?

A. Html, similar but not the same.

Q. Not exactly, but it is the same -- in other words, it is the way that website appears, its fields, that's the php part, right?

A. Yes.

THE COURT: All right. Let's take our mid-morning break now, ladies and gentlemen. And I want to remind you not to talk to anybody else about -- anybody about this case, including each other or anybody else. And we'll come back in just a few minutes. Thank you.

THE CLERK: All rise as the jury leaves.

THE COURT: And, Mr. Kiernan, you can step down and take a break.

THE WITNESS: Thank you.

(Continued on next page)

(Jury and witness not present)

THE COURT: All right. Ladies and gentlemen, let's all be seated.

I want to find out where you're going, Mr. Dratel, because what you can't do with this witness is -- I've allowed, in response to the government's objection about going beyond the scope, I have allowed you some room, but what you can't do is make him into a generalized computer expert for the defense. You are welcome, of course, if you have complied with the appropriate disclosure requirements, to call your own expert or to call a percipient witness. But the mastermind page came in through the back button series. It was a percipient witness set of testimony, as opposed to generalized how you would enter the username. The username was there, but the coding behind it was not the subject of this witness' testimony.

MR. DRATEL: He testified about php. He testified about the website pages.

This is from the laptop. We are going to establish that with him. And it is from the laptop, and he said he looked at php files. He should just --

THE COURT: You have to stay within the scope of the direct. So the direct is not just because he mentioned php, every php question you can think of that might be helpful to the defense, it is to go after what this witness testified about. The scope of his direct, as you know, determines the

parameters of the cross. And so you are welcome to go anywhere with the cross. But his direct was actually quite narrow. It was here's what I got. Here are the files I extracted.

MR. DRATEL: He put in the entire laptop. That is fair game now.

THE COURT: It is not fair game now.

MR. DRATEL: He can't just ignore it by not asking the witness. He examined the entire laptop.

THE COURT: You can get him, through cross-examination, on any one of the files he testified about. Go after that. But you've got to tie it specifically to the file in the extraction process. The two things he did was extraction, and then this file came out of this directory, which had this folder in it. That's it.

MR. DRATEL: No, but there is more. He puts in a whole document, essentially. If someone puts in a 30-page document and he only testifies about page 2, that doesn't put the other 29 off limits, I mean, on cross if they are part of the same document.

THE COURT: Sometimes it does. It depends. And so just because he's got a laptop that he's authenticated doesn't mean he can be your laptop expert.

Now, to be clear -- to be clear, if you want to call somebody to talk about php, the laptop more generally, BitTorrent more generally, that's the defense case, but this

witness is not your generalized computer witness.

MR. DRATEL: He is not an expert. I'm not making him an expert. He testified, number one, about the mastermind page yesterday. And he testified about the mastermind file on the laptop in the php directories. That makes him fair game for --

THE COURT: That does not make him --

MR. DRATEL: I can't be limited to just -- then I have no cross if all I can do is just talk about what they've talked about. Cross is much further than that.

THE COURT: No. What you can do is talk about whether or not in fact the file that he looked at on the computer was not a php file, it was really something else, whether or not his definition of php was inaccurate. You go dig into anything that he testified about. Whether when he pushed the back button it somehow corrupted the file, changed the file, whether or not he's reading the directory and the file paths correctly.

Let me hear from the government, but I am concerned that this is going to go on far longer than it needs to go because you are trying to make him into a different witness.

MR. DRATEL: He answered the question, no, he can. I just want to now establish that it's in the laptop --

THE COURT: I know, but we are going to be coming back to the same problem again and again.

MR. DRATEL: I don't think so.

THE COURT: Let me hear from the government about your

view.

MR. HOWARD: Your Honor, I think the Court has it absolutely right. That is why we are objecting as to the scope of the cross-examination.

Mr. Kiernan simply testified to the extraction of files from certain locations on the laptop. He did not testify about how the scripts worked, how they operated, or anything of that sort. And it is apparent that Mr. Dratel is trying to go further than the scope of Mr. Kiernan's direct, which was just simply about locating and extracting files from the digital evidence.

MR. DRATEL: He didn't. He went further. He talked yesterday about the purpose of php and --

THE COURT: You can go after -- if his definition of php was wrong and you want to undermine his credibility in terms of his expertise by asking him whether the definition is correct, that is fair game. Absolutely. No doubt about it. That is absolutely impeachment material.

If, however, by merely mentioning the word "php" you are now going to find other kinds of php material which would be helpful to the defense, he's not your witness. You need a different witness, either that the government may later call where you can use it or where you yourself call. But we are going to stay within the scope of the direct or this is going to become a detour and frolic. You need to call a witness to

make the points you want to make if it is beyond the scope. I am not going to allow it to be very far afield.

You know what's within the scope of the direct.

MR. DRATEL: I disagree, your Honor. OK. So --

THE COURT: Well, stay within the scope of the direct. And if you are able to stay within the scope of the direct, then it will be clear to us both that you understand what I'm saying. If you continue to go outside the scope of the direct, I will sustain the government's objections.

The government should continue to object if it believes it is outside the scope of the direct. I wanted to see where this was going. It's going outside the scope. I want to say, for the fifth time I think now, I am by no means suggesting that the defense can't put on evidence it believes is appropriate as to these very topics, as to these very documents, as to these very files, but it's for the defense to do if it's not for the purposes of directly going into the scope of the direct of this witness.

Let's take our own break and then we'll come back.

THE CLERK: All rise.

(Recess)

THE COURT: All right. Let's bring out the jury.

(Continued on next page)

THE CLERK: All rise as the jury enters.

(Jury present)

THE COURT: All right, ladies and gentlemen. When you get to your seats, please be seated.

Mr. Dratel, you may continue.

MR. DRATEL: Thank you, your Honor.

BY MR. DRATEL:

Q. So let's go back to your creating those Tor chats, where you create the Tor chat that showed that myself was you, right, on the Tor chat? Do you know what I'm talking about? You testified about that on direct.

A. Yes.

Q. So you set up your computer with Ubuntu, right?

A. Yes.

Q. And Linux, right, which Ubuntu runs on?

A. They run the same, yes.

Q. Do you know how Mr. Ulbricht's laptop was set up, in other words, the methodology of how the Tor chat program was installed?

A. No.

Q. And, in fact, Linux is highly customizable, right, meaning -- withdrawn.

A user who installs Linux has a lot of options, correct?

A. Yes.

Q. And can make a custom version for themselves based on a lot of variables?

MR. HOWARD: Objection to form.

THE COURT: Sustained.

Q. A user of Linux has a lot of options of features to put on their system and how they get on the system, correct?

MR. HOWARD: The same objection, your Honor.

THE COURT: I will allow this one question.

A. Yes. You can customize your install.

Q. And there is something called a kernel, correct, k-e-r-n-e-l?

A. That's correct.

Q. That is an essential part of the Linux operating system?

A. Yes.

Q. And the composition of the kernel is also a critical factor in terms of its customizing, correct?

MR. HOWARD: Objection. Beyond the scope.

THE COURT: Sustained.

MR. DRATEL: Your Honor, he did an experiment --

THE COURT: Sustained.

MR. DRATEL: He --

THE COURT: Sustained.

Q. In your experiment, do you know -- you used a bundle of Linux -- or Tor chat, right? Withdrawn.

Linux is an open-source program, correct?

A. Yes.
Q. It is available for free on the Internet, right?
A. Yes.
Q. And both Linux and Ubuntu are perhaps not as popular as Windows but they're popular, right?
MR. HOWARD: Objection.
THE COURT: Sustained.
Q. The Linux kernel is essentially the glue that holds the software and the hardware together, right, for Linux?
MR. HOWARD: The same objection.
THE COURT: Sustained. Stay within the scope of the direct.
MR. DRATEL: Your Honor, this is within the scope.
THE COURT: Sustained.
MR. DRATEL: Can I have another sidebar, please?
THE COURT: No. Move on to your next line of questioning.
BY MR. DRATEL:
Q. So you don't know if the kernel that Mr. Ulbricht had --
THE COURT: Leave "the kernel."
Q. You used a Tor chat -- withdrawn.
You downloaded Tor chat through something called the Debian package, correct, D-e-b-i-a-n?
A. And AppGet, yes.
Q. I missed that last one.

A. The install command is AppGet.
Q. Oh, OK. But that's a preconfigured package that has all of the Tor chat elements in it and you just put it right in on the machine, right?
A. Yes.
Q. OK. But it can also be done in sort of a DIY, do it yourself, where a user can take code and put it in separately. They don't even have to buy the package as a bundle. They can do it on their own with the various components, correct?
MR. HOWARD: Objection. Beyond the scope and foundation.
THE COURT: Sustained.
MR. DRATEL: Your Honor, it's not beyond the scope.
THE COURT: Sustained.
MR. DRATEL: May I be heard?
THE COURT: No. You can be heard on this at the next break. Go on to your next line of questioning.
BY MR. DRATEL:
Q. So in the experiment that you described yesterday, you don't know that the way that you installed Tor chat on your computer and the version of Tor chat was the same as that on Mr. Ulbricht's computer, right?
A. That's right.
(Continued on next page)

BY MR. DRATEL:

Q. So, the experiment that you ran -- withdrawn.

The purpose of a scientific experiment is to try to replicate as much as possible - and frankly completely - all of the elements of one set of events so that you can match them to a second set, right?

MR. HOWARD: Objection.

THE COURT: Sustained.

Q. If an experiment doesn't have the same elements in it to get to a result, it's not a valid experiment, is it?

THE COURT: Why don't you ask it in terms of the experiment he did.

MR. DRATEL: Yes. That's what I'm trying to do.

THE COURT: No. You're saying "if an experiment." Not any generalized experiment. Talk to him about the experiment he did.

MR. DRATEL: That's what I was doing before. That's exactly what I was doing before.

THE COURT: Try again.

Q. In your experiment, TorChat is an essential element of your experiment, correct?

A. Not essential, but it's -- the download was important to get, yes.

Q. Could you have done it without TorChat?

A. I needed TorChat to run -- it wasn't an experiment. I

wanted to make sure that the log files, what directory they would start in and if logging was enabled by default. Nothing more complicated than that.

Q. You were trying to create a Tor chat so you could see if "myself" was you on the TorChat, correct?

A. That was part of it; yes.

Q. So you needed TorChat for that, right?

A. Yes.

Q. There are different versions of TorChat, correct?

A. I don't know how many versions there are of TorChat.

Q. And you have no idea what version Mr. Ulbricht downloaded?

A. I don't know, no.

Q. And you don't know whether he downloaded it through a Debian package or whether he did it himself by taking components off the Internet and making the TorChat program accessible on his computer, right?

A. That's right.

Q. So, when you do an experiment like that, the experiment that you did, if you don't know what went into it, how can you verify what came out of it?

A. "Myself" is the user of the computer.

Q. On the one that you did, correct?

A. On the one that I did.

Q. And you didn't do it on the one that Mr. Ulbricht's laptop had, right?

A. I didn't do it with the version that he had, or I don't know what version he had on his.
Q. Right.
A. Right; that correct.
Q. Now, Linux -- you talked about creation dates, modification dates, right?
A. Yes.
Q. Linux has timestamps for three times of files, right, three types of timestamps, correct?
A. Yes.
Q. One is an "M" time, right?
A. Correct.
Q. C time, right?
A. Yes.
Q. And "A" time, right. "M" time is for the modification time of a file, right?
A. Yes.
Q. When the content of the file was last modified, right?
A. That's right.
Q. "A" time is for access, right?
A. Yes.
Q. When the last time it was opened or reviewed, right?
A. Accessed.
Q. And "C" time is not creation time, correct, Linux doesn't recognize creation time the same way Windows operating systems

do?
A. It does in the ExT4 version of the file system.
Q. And when did that come out?
A. 2010 I believe.
Q. So do you know what was running on Mr. Ulbricht's?
A. ExT4; yes.
Q. So you're saying that recognized "C" time?
A. Oh, yes.
Q. That was the creation time?
A. Yes.
Q. It's not the last time that metadata associated with the file was changed, that's not what "C" time is in a Linux system?
A. No.
Q. Now, you're familiar with Linux, right, you again have certifications in programs, right?
A. Yes.
Q. And there's an option on Linux called Touch by which you can change -- you can manipulate these metadata times, right?
A. There is. Touch files.
Q. So it doesn't have to -- so when something says "May 8, 2012," that could have been changed somehow by the Touch system, right?
A. You can always change file systems, I mean, times, I mean.
Q. So metadata just tells you a number, right? A date, a

time. It doesn't verify that that's the date something actually happened, correct? Right?

A. It verifies the time that the files were there and created and modified, but those are -- again, they're editable. Sure.

Q. Metadata is editable just like content, right?

A. Correct.

Q. And the Tor chat files are ordinary text files that can be edited even after they're created, right?

A. Yes.

Q. So you talked about MD5 Hash values, right?

A. Yes.

Q. And the files that you took off the computer, you said you had copied a couple of files initially, correct?

A. Yes.

Q. Before you gave it to Mr. Beeson, right?

A. Yes.

Q. And you didn't do any hash values for those, right?

A. No. I don't have any fields.

Q. So just to make clear about the hash values, the hash values you're comparing is not to the laptop itself, correct, it's from the image that Mr. Beeson created, right?

A. It's the hash value from his image.

Q. Right. So it's not from the laptop. It's from the image?

A. The image is from the laptop, right, it's from the image that he created.

Q. The hash value is from his image, right?
A. Correct.
Q. In other words, you're comparing what you copied on your computer to the image you got from him and they matched, right?
A. Yes, yes.
Q. Not from the laptop itself?
A. That's where the image was created from.
Q. But it's not a hash value from the laptop itself?
A. No, not from the laptop itself. That's in a different -- that was on the hard drive that came back that was a brick that we couldn't actually look at.
Q. Now, by the way, as far as encryption goes, on Ubuntu, this -- the encryption that was running is an option on Ubuntu, right?
A. Yes.
Q. So anyone who downloads Ubuntu can use that encryption option?
A. I'm sorry. Say that again.
Q. Anyone who downloads the Ubuntu operating system could avail themselves of that encryption option that was on this machine?
A. Sure.
Q. And you don't know whether closing the laptop would have turned it on, right, made the files unavailable, right? You don't know because you didn't close it, right?

A. We closed it later on, and we weren't able to get to any of the file systems.
Q. And was that -- Mr. Beeson was involved in that?
A. Yes.
Q. So that was really his work, not yours?
A. Well, correct.
Q. Right, so that's what you heard?
MR. DRATEL: I move to strike that, your Honor, as hearsay.
THE COURT: That answer is struck.
Q. Now, with respect to hash values, there can be problems with MD5 Hash values, correct?
A. Yes. There is a one -- there is an older problem with MD5s that it was able to recreate -- it's one of those long shot-type deals that happened -- that was you're able to create a file and make another MD5 with the same number, but with two different files. It's a known problem.
Q. And in fact, there's a better system called SHA1, right?
A. Yes.
Q. And, in fact, if we look at Government Exhibit 205A -- or 201, whichever. Look at 205A or 201. I saw 205A this morning, so that would be easiest.
In fact, there's a section for SHA, right?
A. Yes.
Q. But you didn't do that one. You just did the MD5?

A. Yes. We used the MD5. Standard.
Q. Even though SHA1 is more reliable?
A. They're both very reliable.
Q. SHA1 is more reliable, correct?
A. Yes.
Q. Now, let me talk about some of the exhibits that were admitted through you yesterday. If we can go to 240A, please, if we can scroll up a little bit.

This is a journal entry that you put in, right?

A. Yes.
Q. And it's labeled "2010," correct?
A. Yes.
Q. So if we can go up to the part that the government did not read yesterday. And I'll read it: "Up to this point, I had been working on selling my rental house in Pennsylvania. It had helped me stay afloat with around $600/mo in cashflow, but finally the sale came to a close. I made about $30k off the whole thing, and could finally start trading again. I had been practice trading for a while and saw an opportunity to take my $30k And make it as a day trader. $30k isn’t alot to start with, and I didn’t get off to a very good start with my trading. Around that time, another opportunity came into my life. Donny had gotten a job offer from his brother in Dallas to be the VP of sales at Their milling company. He didn’t know what to do about Good Wagon which he had grown somewhat to the

point that he was making around $6k per month in sales. He made me an offer. 50% of the company and a $3k per month salary to take over and run the business going forward. I took the deal and we went to work on it. By the end of the year, we had our best month on record with about $10k in sales in December."

This is 2010, correct -- go back to the top just for a second -- right?

A. Yes.

Q. So let's go further down, the next highlighted portion, again not read by the government: "I went through a lot over the year in my personal relationships as Well. I had mostly shut myself off from people because I felt ashamed of where my life was. I had left my promising career as a scientist to be an investment adviser and entrepreneur and came up empty handed. More and more my emotions and thoughts were ruling my life and my word was losing power. At some point I finally broke down and realized my love for people again, and started reaching out. Throughout the year I slowly re-cultivated my relationship with my word and started honoring it again."

Let's go to 240B. This is "2011" it says, right?

A. It does.

Q. So let's go to the highlighted portion, again not read by the government yesterday: "At some point, a hacker found some major flaws in my code. I sent it to him for review and he came back with basically “this is amateur shit”. I knew it too. I

tried to work with him but I think he lost interest and since I wasn't charging commission, I only had my shroom money to pay him with. Thankfully that quadrupled from bitcoin increasing in price, little did I know I could've cashed out at 8x higher for a total of 32x! That would have gotten me off to a hell of a start. As it was, I cashed out all the way up and all the way down. I called the peak, my timing was just off."

If we go down further -- no, I think that's it for that. No. Okay. I'm sorry. I just want to ask you a couple of questions while we're talking.

The bitcoin came up. You talked yesterday about cold storage bitcoin, cold storage?

A. I did.

Q. And the bitcoins don't become physical at that point, right?

A. Never physical.

Q. They're always digital, right?

A. That's right.

Q. They're always electronic, they're always in a file, right?

A. Yes.

Q. Or a wallet, let's say, right?

A. Yes.

Q. And transactions cashing out of them are going to be registered on the public block chain, right?

A. That's right.

Q. Let's go up. This is another paragraph or another section not read by the government: "It looked like I didn't have to process the transactions manually anymore, but then the rot started. Some where the site accounting wasn't balancing and I was losing hundreds of dollars every few hours. I started to panic. I tried everything I could think of, but couldn't stop the bleeding. It was getting to the thousands of dollars and I was losing sleep and getting slow. I didn't give up though. I rewrote the entire transaction processor from scratch and some how it worked. To this day I don't know what the problem was."

Now, I want to look at 232A which is a Tor chat. This is March 14, 2012?

A. Yes.

Q. And it's between "da" and it says "myself," right?

A. Yes.

Q. And it says "We might want to construct a new identity for you though," right.

A. That's what it says; yes.

Q. And if you go down further and the person asks "IRL or online."

IRL means in real life?

A. Oh. You're asking?

Q. IRL?

A. Yes. I'm sorry.

Q. "Or online," right? DA is asking "myself," I guess that's

Dread Pirate Roberts, right?

MR. HOWARD: Objection; foundation.

THE COURT: Overruled. Why don't you just reask the question attached to this.

MR. DRATEL: Sure.

Q. IRL to your knowledge is in real life?

A. In real life; yes.

Q. And in this chat, DA asks Dread Pirate Roberts "IRL or online," right?

A. Yes.

Q. Distinguishing the two things, right?

A. Yes.

Q. Real life from online?

THE COURT: Hold on. He can't testify as to what was meant by these people, but he can say what the word "IRL" means to him.

Q. And Dread Pirate Roberts answers no, just online. My concern is that LE, and that's law enforcement, right?

THE COURT: Hold on. He's not going to interpret what the writers meant. He didn't do it yesterday. He's not going to do it today. You can put somebody else on the stand to do that.

Q. "My concern is that LE will see that DA is a player at Silk Road by your forum presence and then track down who you bought from, and sold to under that name and then find you irl."

Now, that application for the Island of Dominica that you looked at yesterday, right --

A. Yes.

Q. -- all of the personal identifying information with respect to Mr. Ulbricht that was in there - name, address, social security - all the things in there was all accurate, wasn't it?

MR. HOWARD: Objection.

THE COURT: Sustained.

Q. Do you know of any of it that was inaccurate?

MR. HOWARD: Objection.

THE COURT: Sustained.

Q. Did you check as to the accuracy of any of that information?

THE COURT: I'll allow that.

A. Personally, no.

Q. And in that document, he provides references, right, persons, correct?

A. Correct.

MR. DRATEL: Nothing further.

THE COURT: Thank you.

Any redirect?

MR. HOWARD: Thirty seconds if you don't mind. It will be very brief, your Honor.

THE COURT: All right. Redirect examination.

REDIRECT EXAMINATION

BY MR. HOWARD:

Q. On cross-examination, you testified about BitTorrent, correct, BitTorrent?

A. I did.

Q. And BitTorrent was on the defendant's computer, correct?

A. It was, yes.

Q. And it's basically a file-sharing program?

A. Yes.

Q. You can --

MR. DRATEL: Objection.

THE COURT: Sustained.

Let's put it this way: You had better state very carefully with only the limited amount that was opened by the defendant. Don't go beyond that.

Q. Did you look at the settings of the BitTorrent program on the defendant's computer?

A. Yes.

Q. Did you see where -- what the settings indicated about where files downloaded to the defendant's computer would go?

A. Yes.

Q. And what folder did that indicate the files would go?

A. The home/frosty/downloads folder.

Q. Did you look at the contents of that folder?

A. Yes.

Q. And what was contained within that folder?

A. Movies, books, things to that nature.
Q. Were any of the files that were admitted as exhibits during your direct examination found in that folder?
A. No.
Q. You testified about the Tor chats on cross-examination, correct?
A. I did.
Q. And you've logged your own Tor chats, is that right?
A. I have.
Q. And have the logs of those Tor chats been true and accurate transcriptions of the Tor chats that you have had?
A. Yes.
Q. And you found the Tor chats we put in on direct examination, you found them on the defendant's computer, correct?
A. I did.
MR. DRATEL: Objection.
THE COURT: Overruled.
You may proceed.
A. Yes.
Q. You testified on direct that you found encryption -- an encryption process was active on the computer, correct?
A. Correct, yes.
Q. If the defendant had been able to close his computer before he was arrested, would you have been able to access the Tor

chat files?

MR. DRATEL: Objection; objection.

THE COURT: I will allow it.

A. No.

MR. HOWARD: Let me check with cocounsel and see if there's anything else, but I think we're done.

No further questions.

THE COURT: Mr. Dratel.

RECROSS EXAMINATION

BY MR. DRATEL:

Q. To be clear about the last point, you didn't close the laptop, correct?

A. Correct.

Q. So you don't have any personal knowledge as to what would have happened had that laptop been closed, right?

A. I know when I got it back --

Q. No.

A. Personal, no.

MR. HOWARD: No further questions.

THE COURT: He may still be going.

MR. HOWARD: Pardon me.

Q. Now, you testified about BitTorrent on redirect about files, about download destination, right?

A. Yes.

Q. But you can't sit here now and testify that you know all of

the activity that went on through that open port on that computer, either that day or some other day when he was downloading something else?
A. Not from the whole time period.
Q. Right.
A. But that's a BitTorrent --
Q. But that's a BitTorrent, but the port is open and it gives access to the computer, correct?
A. It gives access to the BitTorrent client.
Q. Right. But people who -- and that means those seven users out there who have it, right, who are connected?
A. That's right.
Q. And as we said before, it could contain all sorts -- that anything you download, can contain all sorts of malware, right, malicious --
A. Possible.
Q. -- malicious software that can be used against the person who is operating the computer, right?
MR. HOWARD: Objection.
THE COURT: Sustained.
MR. DRATEL: I have nothing further.
THE COURT: Thank you.
Anything further, Mr. Howard, like one question?
MR. HOWARD: Yes. It is one question -- two questions, but start with one.

REDIRECT EXAMINATION

BY MR. HOWARD:

Q. Mr. Kiernan, did you review the contents of the defendant's computer for malware?

A. Yes.

Q. Did you find any --

THE COURT: I stopped Mr. Dratel on the malware.

MR. HOWARD: I'm sorry. Withdrawn. No further questions.

THE COURT: Thank you.

You may step down.

THE WITNESS: Thank you.

(Witness excused)

THE COURT: Would the government like to call its next witness, please.

MR. HOWARD: The government is calling Special Agent Greg Fine. We're getting him right now.

(Witness sworn)

THE COURT: Mr. Fine, please be seated. And it will be important for you to pull up your chair and adjust the microphone so that you can speak clearly and directly into the mic.

THE WITNESS: Thank you.

THE COURT: Mr. Turner, you may proceed.

MR. TURNER: Thank you.

CROSS EXAMINATION

MR. DRATEL

Q. Good afternoon, Mr. Shaw.

A. Good afternoon.

Q. I want to go back to Government Exhibit 901 which you testified about on Thursday with respect to an SSH key.

A. Yes. Okay.

Q. And that's in evidence and there were two SSH keys on the Silk Road server, correct?

A. Correct.

Q. And there was one ending in frosty@frosty and one ending in root@bcw, right?

A. Correct.

Q. And an SSH key essentially allows someone to have remote administrative access to a computer server?

A. Correct.

Q. And by administrative access that means total control over the site, right? Through those keys?

A. Correct.

Q. Not just general administrative access but through these SSH keys, correct?

A. Correct. In this case, correct.

Q. So, an individual gaining access through those SSH keys would be able to review and change any information in the server, correct?

A. The database had its own authentication which would be separate, but otherwise, correct.

Q. And anyone getting in through that SSH key would be able to obtain information that's logged within the database or on the server, correct?

A. Again, the database had its own authentication, but yes, correct.

Q. And that would include they could get login and password information for the Dread Pirate Roberts account, right?

A. Depends on which -- what you mean by password information. Passwords are typically stored

encrypted.

Q. Well, but typically, but do you know?

A. I'm sorry?

Q. Do you know though, with respect to that? With respect to the server?
permalink

Page 1972
A. It is the default for the ubuntu which the server was.

Q. Do you know?

A. And then for the --

Q. The question is do you know.

A. Can you rephrase your question, please?

Q. Sure.

You said that typically such information would be encrypted. Do you know for a fact whether that information, DPR's password and login information on the server, was encrypted?

A. I have not verified that.

Q. Now, so, by the way, with respect to, you had, on Government Exhibit -- the mastermind page for the server, right?

A. Yes.

Q. And if you log in as Dread Pirate Roberts that automatically comes up, correct?

A. No, it does not. It depends which page you come from. There are two login pages.

Q. So which login page does it come up on automatically?

A. There was a special support admin login page.

Q. For the support admin page, right?

A. Correct.

Q. And you testified Thursday that you used both an MD5 hash value and an SHA 1 -- you call it a SHA 1 or SHA?

Page 1973
A. Shah 1.

Q. So, MD5 hash and Shah 1 hash value to confirm the copies of the server that you viewed, right?

A. Correct.

Q. And you did that to ensure that you were looking at the same data that was on the original that you had imaged on a copy?

A. Correct.

Q. There was a reason -- withdrawn.

You used both the MD5 hash and the Shaw 1 hash because you wanted to be thorough and you wanted to be as -- you want to be as reliable as possible, right?

A. It was the default setting for the tool that I used so it automatically calculated both for verification.

Q. But it calculates both but you matched both, right?

A. That's correct.

Q. That's not always -- you don't have to match both, you decided to match both, right?

A. Yes, I did match both.

Q. Not because you wanted to be forensically sound in your analysis, right?

A. Sure.

Q. That's because MD5 hashes have some vulnerability, correct?

A. Depends on the use case.

Page 1974
Q. But you use a SHA 1 because that has more reliability, right?

A. Again, depends on the use case.

Q. But you did it in this case, correct?

A. Because it was available to me, yes.

Q. Now, going back to Government Exhibit 901 and looking at the key that ends the SSH key which we were just talking about -- let me know when you get there.

A. Thanks.

Q. Looking at the key that ends in frosty@frosty and you testified Thursday, I think, that the user name frosty and the computer name "frosty" that are found in the SSH key are taken from the system that you

are coming from?

A. That's correct.

Q. Well, the part of the key that contains frosty@frosty is what is called a comment, right?

A. I don't know that for sure.

Q. Well, you can generate a key ending in frosty@frosty from my computer, right? You can do it at any computer, can't you?

A. That is correct.

Q. Are you familiar with the program called SSH- -- withdrawn.

And you also talked a little bit about on direct on how SSH keys work, right?

A. Correct.

Q. And you are familiar with how they're generated?

A. Yes.

Q. And you have a lot of background and training in UNIX and Linux programs, the two computer systems, right?

A. I have experience at both, yes.

Q. And you are familiar with the manual pages associated with computer programs contained in UNIX-based operating systems like Macrolex or Linux?

A. Yes.

Q. And these manuals contain documentation for how the software works, right?

A. Correct.

Q. And they're widely accepted in the community as being reliable authority on how computer programs contained in a UNIX-based operating system work, right?

A. As long as updated, yes.

Q. And if you look at 901, that's a file called authorized keys, right?

A. Correct.

Q. And that file is associated with a computer program called SSHD or open SSH Daemon, right?

A. I believe that is correct.

Q. And are you familiar with the system manager's manual for that computer program SSHD?

A. I have not reviewed that manual, no.

Q. Isn't the comment field not used for anything other than the convenience of the user to identify the key?

Page 1976
A. Again, I don't know if that is referred to as a comment field or not. I have not reviewed the page on that.

Q. With respect to the Silk Road market server image that you worked on, right?

A. Yes.

Q. There was an image of the server captured October 8, 2013; correct?

A. Correct.

Q. And you received the Silk Road marketplace server by recreating a local copy of the server on your computer, right?

A. Correct.

Q. And just for purposes of shorthand, that was the server ending in the IP address, last two digits .49, right?

A. I don't remember the IP address off the top of my head.

Q. Let's look at 603A -- Government Exhibit 603A.

This is the image that you used to create a local copy of the Silk Road marketplace on your computer, right? In other words this is the log entry?

A. That looks familiar. Correct.

Q. And if you look at the created date on the top -- I'm sorry, on the left as you go down it says: Task, status and created date is Tuesday, October 8, 2013, right?

A. That's what it says. Yes.

Q. And the image that you get is essentially -- not essentially, the image that you get is a snapshot of what exists on the computer at that moment in time, right?

Page 1977
A. Correct.

Q. Now, I want to direct your attention back to Government Exhibit 936, please. If we look at the third entry in the second paragraph, the one that begins on March 14, 2013 at 11:26, right?

A. Okay.

Q. If you look at the second paragraph of that and at first it says -- it says it is from friendlychemist:

"u dont know me but i am lucydrops supplier. the only reason i lent lucydrop so much product is bcuz he showed me the chat logs of u and him talking and how u made him the #1 seller on silkroad."

Now, do you know whether that is accurate or not, that statement?

MR. HOWARD

Objection.

THE COURT

Overruled.

THE WITNESS

I do not know.

THE COURT

I take it by that you mean did he see it, a reference to that elsewhere?

MR. DRATEL

Right.

THE COURT

Was that the question?

MR. DRATEL

Yes, your Honor.

THE COURT

Is that how you understood the question?

THE WITNESS

Yes.

THE COURT

Yes?

THE WITNESS

Yes.

THE COURT

All right.

MR. DRATEL

Q. Further down that entry do you see the paragraph that begins:

"i put a keylogger on lucydrops computer when he left the room one day"...

Right? Do you see that?

A. Yes.

Q. So, when you were looking at hacking software, right, which you showed us on Thursday as well, can you explain what a key logger is?

MR. HOWARD

Objection. Beyond the scope.

THE COURT

Sustained.

MR. DRATEL

Your Honor, the government read this document.

THE COURT

No, they can read the document, but whether or not he knows about how to interpret the content is different. So, you can ask him about the matters that he went over in his direct.

MR. DRATEL

Your Honor, he also testified about hacking software such as that, key loggers, in his direct.

THE COURT

If he talked about it then certainly you can go into that. Don't tie it to the document but go ahead and

question him about things he otherwise testified to.

Page 1979
MR. DRATEL

Q. In terms of hacking software, what does a key logger do?

A. Key logger? It is my understanding that it logs your key strokes.

Q. When you say logs your key strokes, you mean for someone -- it could be done by someone who is not at the computer, correct?

MR. HOWARD

Your Honor, objection. Beyond the scope.

THE COURT

You know, Joe, my LiveNote has gone out.

I will allow this to the extent -- I can't look and see what he testified to on direct as to this topic because my LiveNote is not currently working.

MR. HOWARD

Your Honor, if we can have a side bar we can make a proffer as to that or maybe he could move on to a different issue and come back once you can verify that.

THE COURT

We can do it even more easily. Why don't you say do you recall testifying on direct that? And then that will remind me and it will have the benefit of reminding everybody and then we can take it from there.

MR. DRATEL

Q. Do you recall testifying on direct about hacking tools and reading from the screen pages about what hacking tools were available on Silk Road?

Page 1980
MR. HOWARD

Objection.

THE COURT

Well, that question he can answer.

THE WITNESS

I didn't read out loud any of the hacking tools. I described that there were listings for items referred to as hacking tools.

Q. Known as key loggers, right?

A. That is correct.

Q. So, when you say a key logger logs strokes, it is not by the person who is actually logging them, right? It is someone who wants to know what the person, as a hacking tool -- it is for someone who wants to know what the person is doing on the computer while the person who wants to know is not there, right?

MR. HOWARD

Objection to scope and foundation and form.

THE COURT

Now it is sustained.

MR. DRATEL

Q. Now, let's go to page 8, please, of 936.

That blue portion, that's not from the chats, right?

A. On this page, that is correct, it is not from the chats.

Q. And all blue portions for the entire document are not from the chats, right?

A. They are not from the marketplace chats, that's correct.

Q. They are from the forum, correct?

A. From a file -- backup file from the forum, correct.

Q. And that forum is available to the entire Silk Road community, correct?

A. That is my understanding. Correct.

Q. And it is imported into this document, correct?

A. Correct.

Q. So, when we are looking at the -- so, when this was taken off the server, that blue part wasn't there in that chat, right?

A. It was not blue. That is correct.

Q. No, but it wasn't there.

A. Wasn't where? I'm sorry.

Q. In other words, the next entry on the chat is the next white entry, not the next blue entry; correct?

In other words let's parse this out. Let's go to the entry right above it, 3/15/2013 at 20:42, right?

A. Yes.

Q. And that's 8:42 p.m., correct?

A. Correct.

Q. We are talking military time here, right? 24-hour clock.

Okay, so then we have a blue section and then we have another blue section on page 9, right? All blue, right?

A. Correct.

Q. And then we have 10 which is all blue again, right?

A. Correct.

Q. And then we have 11 which is all blue, right?
permalink

Page 1982
A. Correct.

Q. And then we have 12 which is all blue?

A. Correct.

Q. And we have a part of 13 that is all blue?

A. Correct.

Q. Then we have 3/21/2013 at 1:33, that's the next white entry, correct?

A. Correct.

Q. And, in fact, that white entry is the next entry on the private message chat, correct?

A. On the -- yeah, the Silk Road marketplace, correct.

Q. So, all that blue stuff was imported into this document, correct?

A. Correct.

Q. So, if I were to print out just the part that is white I would not see any blue. This was created for purposes of the trial, right?

A. It was the weaving of two different.

Q. It was created for the trial, right?

A. Correct.

Q. Did you do it?

A. I participated in the creation of this, yes.

Q. It is actually occurring on a public forum -- when I say public I mean for any Silk Road user, anyone with a user account, anyone with a user name, anyone with access to the Silk Road site, right?

Page 1983
A. There is the one individual forum post on page 8 and then the rest were one-on-one messages.

Q. But on the forum page?

A. On the forum site, correct, the separate site.

Q. If you go to page 16, 3/26/2013, that second, the third entry, the second white entry at 20:08, right? And it says:

"That is interesting."

This is from redandwhite, right?

A. Correct.

Q. And it says:

"That is interesting. How much is it possible to sell on here if we listed every product far cheaper than everyone else? We have a majority hold over most of the movement of products in western Canada (one of the main drug ports to North America)."

It says that, right?

A. Yes, it does.

Q. Now, if we go to page 17 at March 27, 2013 at 23:38.

Do you see that entry?

A. Yes, I do.

Q. By the way, that blue one in the middle there again, that belongs on the Silk Road forum, right?

A. Right. That is a message on the Silk Road forum, correct.

Q. Okay, that paragraph:

Page 1984
"In those categories, I think you could be doing over $1M in sales a week within a few months. It is hard to estimate because it depends on how much market share you get and also the site as a whole is constantly growing. You will need to become very proficient at stealth shipping and packaging if you aren't already. Think vacuum sealers and leaving no forensic evidence on your packages. You will also want to ship from multiple drop points so you can't be traced back via your (fake) return address.

If you go through with this, I would contact some of the top vendors and hire them to consult you. Ask the weed vendors because you won't be competing with them and their product is smelly and looked for by USPS" --

That would be the United States Postal Service?

MR. HOWARD

Objection.

THE COURT

Sustained.

Q. -- "so they have to be on top of their game."

MR. HOWARD

Objection to form.

Q. It says that, right?

THE COURT

Yeah. What is the objection?

MR. HOWARD

I thought that was the question. I didn't realize.

THE COURT

Do those words appear on the page?

THE WITNESS

Yes, they do.

THE COURT

All right.

Page 1985
MR. DRATEL

Q. That is talking about security, correct?

MR. HOWARD

Objection.

THE COURT

Sustained.

He can't talk about what the content means. He can talk about what the content is on the page but he can't interpret the content. So, move on.

MR. DRATEL

Your Honor, this is a witness who put the document in evidence.

THE COURT

He did. He did put it in evidence. He can't interpret what the people meant.

MR. DRATEL

Q. Let's go to April 2nd, 2013 at 20:55, page 24.

A. Okay.

Q. And that entry which is in the middle of the page, if we can blow that up a little bit it says:

"Regarding image metadata, you can strip all of that out and it is a good practice. The upload page is secure, but I would still have access to that metadata."

By the way, this is from Dread Pirate Roberts to redandwhite?

A. Correct.

Q. So:

"Regarding image metadata, you can strip all of that out and it is a good practice. The upload page is secure, but I would still have access to that metadata. Of course you can trust me, but what if I was compromised? Do a search of 'remove image metadata.' A decent one for windows can be found here:"

Page 1986
And there is a URL, correct?

A. Correct.

Q. "Regarding bitcoin withdrawal, I would avoid mt gox if at all possible, especially if you are withdrawing to a USA account. There are many other exchanges that don't have so much attention on them."

It says that, right?

A. Yes, it does.

Q. And if you look at the bottom, April 4, 2013, that one it says:

"I can't find a surname anywhere of Lawsry."

L-A-W-S-R-Y?

A. Yes, it says that.

Q. In fact, you heard the stipulation, right, that there was no person by that name?

MR. HOWARD

Objection.

THE COURT

Sustained.

MR. DRATEL

Q. Now, let's go to 4/6/2013 on page 26 at 57 minutes, so that would be 12:57, right, after midnight?

A. Correct.

Page 1987
Q. 12:57 a.m., right?

A. Correct.

Q. And just look at that, we will go to the third sentence:

"He is likely sitting on many thousands of stolen bitcoins perhaps tens of thousands, so I would think

we'd want to "work him over" to get those funds back. They could be on an encrypted drive only he can unlock."

Right? It says that?

A. Yes, it does.

Q. Now, from your knowledge of the server, having reviewed the server and the private messages, is there any way for you to tell whether or not lucydrop, redandwhite, reallucydrop, friendlychemist, whether they're different people or the same people?

A. There is -- no. Not that I can think of.

Q. Now, this set of messages occurs from March -- from page 1 is March 13, 2013, right?

A. Correct.

Q. And goes up to April 18th, 2013 -- actually, April 21st, and then there is one also on June 1st, but the particular string is pretty much through April 21st, right?

A. Correct.

Q. Going back to the SSH key for a second, that was changed March 26, 2013? Is that right?

THE COURT

I'm sorry, could you have the court reporter read back the question? I missed it.

Page 1988
MR. DRATEL

I can rephrase it.

THE COURT

Either way. My LiveNote is still not up, we are trying to fix it.

MR. DRATEL

Q. Going back to the SSH keys, you testified, I believe on Thursday, that it was modified -- the frosty@frosty was modified March 26, 2013, right?

A. Can you tell me which exhibit that was, please?

Q. I think it is 603.

A. 900s, hopefully.

Q. 901?

A. Thanks. That is correct; recorded date modified was March 26, 2013.

THE COURT

I am back in business here with LiveNote.

Mr. Dratel, I think you got an answer.

MR. DRATEL

Thank you, your Honor.

MR. DRATEL

Q. If we can go to Government Exhibit 1201?

MR. HOWARD

Objection, your Honor. This has not been admitted into evidence.

THE COURT

Take it down and let's find out if it was.

MR. DRATEL

It may not be, your Honor. It was not the one I was looking for.

THE COURT

So you are looking for a different exhibit?

MR. DRATEL

Q. Government Exhibit 1200, that is in evidence; just look at the date on that, does it say March 16th?

A. Yes, it does.

Q. 2013?

A. Yes.

MR. HOWARD

Objection, your Honor. This is argumentative.

THE COURT

Well, I don't know where it is going yet, so overruled. Let me see where it is going.

MR. DRATEL

It is precisely what the government does in all of its examinations.

THE COURT

Let's see where it goes. I am overruling the objection. Go ahead.

MR. DRATEL

Q. I am saying that this is March 16, 2013, right; and there is a post by frosty to stackoverflow, right, about code, correct?

A. I'm not familiar with this exhibit but it is what it looks like, yes.

Q. Then if we go to the next entry in this exhibit, if we go up further, okay, if we go to -- that's March 16, 2013 and the last modification of the authorized user key for the 16789SH was March 26, 2013, correct?

A. Correct.

Q. And you don't know what it was before then because you just have what it was changed -- what became of it as of March 26, 2013, right?

A. That is correct.

Q. With respect to 940A that is in evidence, you said that the null category was not included in your analysis?

A. It is included in Exhibit 940 -- or 940A.

Q. 940As it included, but when you did the pie chart you didn't include it, correct?

A. That is correct.

Q. And so, the null transactions account for about 11 or 12 percent of the entirety, right, of the transactions?

A. Doing a quick double-check here. That's approximately correct.

Q. And the reason they're null, just again, is because you could not categorize them, correct?

A. That is correct.

Q. Let's talk about 940D and the total number of commissions over the life the Silk Road is 642,455

bitcoin, right?

A. That's what it says. Correct.

Q. And the dollar value of $13 million is based on the value of bitcoin at the time of the transaction, correct?

A. As it was recorded in the database.

Q. So, in other words, if the database recorded bitcoin value, let's say, in 2012, bitcoin value might be different in 2013, correct?

Page 1991
A. Correct.

Q. And that would influence not the value -- not the number of bitcoin but in fact the value of the money, correct, in terms of exchange into dollars, right?

Let me pose it a simpler way for everybody's benefit, including mine.

If a transaction in October of 2012 is 1 bitcoin is worth $4.50, right, that would look there at 1 bitcoin and at the bottom, U.S. equivalent would be $4.50, right?

A. Correct.

Q. If that same transaction occurred with bitcoin at a value of $12 a bitcoin, it would still be 1 bitcoin on the commissions but the dollar value -- U.S. dollar equivalent would be $12, right?

A. That's what the database would -- should reflect, yes.

Q. And so that the database only reflects the value of bitcoin in the transaction, correct? Right?

A. Correct.

Q. Did you look at the value of bitcoin over time?

A. No. I was pulling it from the database. The value recorded in the database.

Q. Let me show you what is in evidence as Defendant's Exhibit B. It is in evidence. This is a graph of the value of bitcoin over time and so in the context of your chart which is 940D, it doesn't tell you what the value is of those commission bitcoins at any point in time other than what is in the database at the time of the transaction, correct?

Page 1992

A. It tells you what the value was recorded in the database.

Q. Right; but it doesn't tell you what happens a month or a year later if those bitcoins are still held and whether the price has appreciated. It is not reflected in that chart?

A. Yes. To my understanding that that field does not change, correct, once entered in.

Q. So that if you had 100 bitcoins at a dollar, right, and in 2012 and you held on to them until November 2013 as on that graph when it peaks at, and we will say $1,000, just for round numbers, that 100 bitcoins at a dollar each would be worth a thousand times more, correct?

MR. HOWARD

Objection. Beyond the scope.

THE COURT

Well, no. It is, I think, related to what he was saying before but I think it has been asked and answered. But, I will allow this last question.

MR. DRATEL

Thank you, your Honor.

THE WITNESS

Yeah, the value of the bitcoin varies wildly.

MR. DRATEL

Q. And it would be a thousand times more but it wouldn't be reflected on 940B?

Page 1993
A. It is my understanding, yeah, that the value in the database did not change.

Q. I want to draw your attention to Government Exhibit 935. If you look at that first entry, this is from shefoundme to KingofClubs, June 10th, 2013. Right?

A. Correct.

(Continued on next page)

Page 1994
Q. And you testified about this Thursday?

A. Correct.

Q. And this is about shefoundme ordering fake IDs, right?

MR. HOWARD

Objection.

THE COURT

Hold on. Well, I think the document says what it says. I don't want the witness to be interpreting it, but if you want to read something into the record, you can do that.

MR. DRATEL

Okay.

Q. Let's read from the top "Hi I need a few of your highest quality IDs. I notice several attributes you list: Hologram, UV, scannable, raised lettering. Can you give me a rundown of the importance of these attributes and what they are needed for? For example, which are needed to pass airport security for a domestic flight?"

Right?

A. Yes, it says that.

Q. "Which are needed to get through being pulled over by a cop." Right?

A. Yes.

Q. And if you go to page two, again, from shefoundme to -- June 10, 2013, shefoundme to KingOfClubs, right?

A. Correct.

Q. And then if you look at the third-to-the-last paragraph down at the bottom, it's a one-line paragraph, "Can you comment on the suitability of using any of these IDs to board a domestic USA flight." Right?

A. Yes, it says that.

Q. Then it says "Can you please comment on what the various attributes mean. For example, does UV mean if it is held under a UV light then some pattern appears that makes it look legit. If it doesn't have UV, does that mean if it is held under UV light, it will be exposed as a fake? In general, how much scrutiny can these cards hold up

against?"

Right?

A. Yes.

Q. Now, if we go to page 11, July 18, 2013, the one right in the middle of page 132606, right?

A. Okay.

Q. From shefoundme to KingOfClubs: "Looks like it got stuck in customs. The last step is 'inbound out of customs' on the tenth. Have you ever had something seized or any of your customers get in trouble?"

Right it says that?

A. Yes, it does.

MR. DRATEL

May I have a moment, your Honor.

THE COURT

Yes.

Q. With respect to SSH keys and what we talked about before with respect to a manual, right, the system manager's manual, are you familiar with them?

A. I'm familiar with man pages in general.

Q. So are you familiar with the SSH-D system manager's manual?

A. I have not reviewed that one; no.

Q. But you testified here about SSH keys, right?

A. That is correct.

MR. DRATEL

Nothing further. Thank you.

THE COURT

All right. Thank you.

Mr. Howard.

MR. HOWARD

I'll be very brief.

THE COURT

All right.

MR. HOWARD

Mr. Evert, can you please publish Government Exhibit 936 again, please.

REDIRECT EXAMINATION

MR. HOWARD

Q. Mr. Shaw, this is a compilation of messages involving the Dread Pirate Roberts, correct, other than the forum posts?

A. That's correct.

Q. Can we go to page seven, please. And the one that's shaded here on blue on page eight, that's the forum post, right?

A. That is correct.

Q. A forum post can be seen by many users on Silk Road, right?

A. That's correct.

Q. Can we go to the next page. Isn't it true that you testified that all of the other messages shaded in blue were private messages taken from the forum database, correct?

A. That's correct.

Q. Those are one-to-one private messages involving Dread Pirate Roberts, correct?

A. Correct.

Q. So 936, apart from that forum post, contains private messages taken from the private

message database on the Marketplace, correct?

A. Correct.

Q. And also private messages between Dread Pirate Roberts and other individuals taken from the forum database?

A. Correct.

Q. And all of these were contained on the servers you reviewed?

A. Yes, they were.

Q. You testified about MD5s and SHA1s on cross, right?

A. Yes, I did.

Q. And you testified that whether or not you used one or both comes down to the use case, correct?

A. Correct.

Q. What do you mean by "use case"?

A. For the purposes -- there are multiple use cases for hashing a file. Typically in the forensic world, users will create what's called a white list, you know, known files. And so it's common to create hash values of those files so that way, you know, every Windows computer ever has notepad.exe, so if you create a hash value of that file, whenever you import your new image, you can quickly exclude that image. So it's a process for quickly excluding files. So it's fairly common to use hash values to eliminate files that need review and there was, you know, a few years ago some academic papers and studies on weaknesses in MD5 for that purpose.

Page 1998
Q. So for the purpose of creating forensic images, however, are you aware of weaknesses in MD5?

A. For comparing whether a file has changed, you know, whether it's been under control and whether it's changed from point A and point B, MD5 is still used; yes.

Q. So relying on MD5 alone would be sufficient?

MR. DRATEL

Objection.

THE COURT

Sustained.

You can ask a different way.

Q. Is MD5 alone accepted in the community as a way of verifying forensic copies?

MR. DRATEL

Objection; form.

THE COURT

I'll allow it.

A. MD5 is a -- still considered a technique for verifying if a file changed in transit. With hash values, if they're -- that weakness that I discussed, something else will also change in the process. So the size of the file will likely change almost always will get larger. Additionally, if it's, like, a jpeg type image, that the image would get corrupted. So when it comes to verifying whether a file changed in transit, it's still considered a valid process.

MR. HOWARD

No further questions, your Honor.

THE COURT

Mr. Dratel.

RECROSS EXAMINATION

MR. DRATEL

Q. It's not most valid process, though, is it, right? SHA1 is more reliable than MD5?

A. SHA1 is the newer standard that --

Q. I'm sorry --

A. The newer process that doesn't have the same weakness as MD5.

Q. And with respect to the 936 of those posts, those were -- the blue sections were imported from a different -- that's a separate conversation going on from the white ones, right --

A. That is correct.

Q. -- in terms of where it's occurring?

A. Correct.

MR. DRATEL

Thank you. Nothing further.

CROSS-EXAMINATION

MR. DRATEL

Q. Mr. Yum, the analysis that you spent on the bitcoin wallet analysis that you've been talking about for the latter part of your testimony, you began that within the last two weeks?

A. A little less than two weeks.

Q. And you said you worked with one other person on it?

A. Yes.

Page 1733
Q. Who was that?

A. It's a colleague of mine.

Q. And what is his name?

A. Mathew Edmond.

Q. And what's his -- what are his credentials?

A. He has a doctorate in cryptology.

Q. What did he do as part of this project?

A. He worked with me to identify the wallets, extract the bitcoin addresses, and compare that to the block chain.

Q. Did he do that actual work?

A. We both did.

Q. So he did some of that work?

A. Yes.

Q. Correct?

How many hours did he put into that?

A. We both worked on it for about a week together, so I think we're a little short of 100 hours. He put in about 60. I put in about 40.

Q. And what were his contributions to Government Exhibit 620 which is the spreadsheet, the large spreadsheet with all of the transactions. Right, isn't that the --

A. Yes.

Q. So what's his contribution to that?

A. He assisted me in obtaining the underlying raw information for that summary.

Page 1734
Q. And how was that exhibit created?

A. That one? I believe I just summarized the Excel file, so that's an Excel spreadsheet. I took all of the raw data and created a summary chart on Excel.

Q. But in terms of the matching, did you use any software to match the transactions?

A. Oh, the actual analysis?

Q. Yes.

A. Yeah, we loaded all the information onto a table and did a query on that table to find the matching transactions.

Q. And what program?

A. I believe the actual matching was done through Python.

Q. And what is Python?

A. Python. It's a scripting language.

Q. Did you have any participation in writing the code for that program?

A. Actual hands-on typing was done by Mr. Edmond, but we both sat down to work out the logic.

Q. But I mean in terms of the program itself, did you create that program?

A. Oh, no. So the reason why we use Python is there's available software called Pie Wallet, which was also found on the defendant's laptop, it's a common Python application that's used to manage bitcoins. So we used commands that are commonly used by all the bitcoin users.

Page 1735
Q. And you don't have any notes of the work that you did?

A. It's back in my office.

Q. You do have notes?

A. Well, the program itself.

Q. So you have notes of what you went through to accomplish this, right?

A. It would be the logic within the matching.

Q. And it was important for you to have help in this project, right?

A. In the amount of time that we needed to do the analysis, yes.

Q. Well, could a layperson have done it just running off the top of their head?

A. It may be time-consuming, but every information that we used, well, we had the public addresses for all of the defendant's laptop, so that's not available to the public but we have it because the private keys were found in his laptop.

Q. But we had someone with a doctorate, correct, in cryptology working on this project with you, right?

A. Right, it's easy as going to blockchain.info and typing those addresses to see if you could locate a transaction that you see --

Q. And how long would it take you to type in all of the addresses?

A. It's time-consuming. That's why we had two people working on it.

Page 1736
Q. Figure with two people, you would have done it in a week without any of the computer work that you did, without any of your knowledge and experience that you bring to the project?

A. As a manual process, no. You can't do that as a manual process.

Q. So then my question is -- withdrawn. So you do have notes and a progression of what you did, right?

A. Well, the notes would be the files on the computer where this analysis was done.

Q. Now, when you seized the bitcoins from the servers, right, in fact, the FBI didn't even have a protocol for establishing a wallet where to put seized bitcoins, right?

A. Correct.

Q. You had to create that?

A. Yes.

Q. You talked about the concept of a wallet, right, multiple wallets, multiple wallets and multiple addresses within wallets, right?

A. Right.

Q. You know what I'm talking about. So, you can't tell where a particular wallet was created, correct?

A. Correct.

Q. It can move from computer to computer, correct?

A. Yes, it can.

Page 1737
Q. And you can also move an address from one wallet to another wallet, correct?

A. Yes, you can.

Q. So you can't say how long any of the addresses of the wallets were on Mr. Ulbricht's computer other than the day he was arrested, right?

A. Can you repeat the question.

Q. Sure. You can't say when other than the day that Mr. Ulbricht was arrested or if those wallets or those addresses were on that laptop, other than the day he was arrested?

A. Yes, but there -- the wallet files are computer files in itself. So there is a last-access date of that file. And some of them dated prior to the day of the arrest. Some, months prior; some, weeks prior.

Q. Now, also the wallet that the bitcoins were in on Mr. Ulbricht's laptop, the 144,000 bitcoins, right --

A. Right.

Q. -- that was a hot wallet, right, as opposed to a cold storage wallet, right? It had the bitcoin program in it. It was a hot wallet by definition, right?

A. It's only hot if it's online. And the wallet that contained the most number of keys on the defendant's laptop, I don't believe that was synchronized to the block chain until August.

Page 1738
Q. I'm not talking about keys. I'm talking about bitcoins themselves.

Bitcoins themselves, the wallets -- the addresses within the wallets that the bitcoin were in, they were basically in one wallet, correct?

A. The majority came from one wallet.

Q. Right. And that wallet had a bitcoin program running in it, right?

A. Yes, but the program hasn't run since August of 2013, so -- it will be a cold wallet at that point.

Q. But isn't a cold wallet where it's not connected to a program where you can actually take the wallet, put it in a file or in a folder or somewhere else on the computer and extract the program -- extract it from the program so that it can't execute any functions, right?

A. Well, a cold wallet is something that's not online. So if the wallet's last access date was August 2013, it hasn't been online since August 2013; therefore, from August until October, it's a cold wallet because

it never went online.

Q. But it still has a program in it, right, and it's still capable of execution?

A. Right, but it didn't execute because it would have updated that last-access date on the wallet.

Q. But if someone doesn't use their wallet, it doesn't mean it's a cold wallet; it can still be a hot wallet. You're just not using it, right?

Page 1739
A. No, not correct.

MR. TURNER

Objection; asked and answered.

THE COURT

I'll allow it.

A. A hot wallet is a wallet that is currently connected to the Internet.

Q. At that time? At the very time?

A. At the very time.

Q. That's your definition?

A. Yes, it is.

Q. Okay. And how many bitcoin cases did you have before this one?

A. This was a second case I believe.

Q. Now, you talked about identifying servers and identifying bitcoin server, right, and identifying the servers from the Philadelphia servers, right?

A. Right.

Q. You testified about that. What you saw from the code was only an onion address, right? In other words, looking back to find the servers, correct, it wasn't an IP address. It was --

A. I'm sorry. Which address and which server are you referring to?

Q. The server to which the backup data was exported to the jtan -- the Philadelphia server, right?

A. Correct.

Page 1740

Q. From the Iceland server, right?

A. Yes.

Q. Now, what you saw there when you're looking to find that is an onion address, right, an onion url, dot-onion url, correct?

A. I was brought onto the case around that time, and I received an IP address. And my -- the investigative team, before I joined, they were the ones who did the analysis, so I can't speak to what allowed me to receive that IP address, but I received that IP address. Nothing else.

Q. Now, the servers were first -- you went in October to Iceland, correct?

A. Correct.

Q. And to be there at the time of the arrest to shut down the servers, correct?

A. Yes.

Q. And to put the seizure banner up, we saw at Exhibit 600, right?

A. Right.

Q. The government had access to the servers -- the U.S. government had access to the servers in July of 2013, correct?

A. That's what I've been told --

MR. TURNER

Objection; foundation.

THE COURT

Sustained.

Q. Now, isn't it true that a Silk Road user would have communications -- withdrawn.

A Silk Road user would have transactions with the Silk Road wallet, correct, and their own wallets, right?

MR. HOWARD

Objection; beyond the scope.

THE COURT

Overruled.

A. I'm sorry. Can you clarify.

THE COURT

Let's not make a hypothetical. Why don't you ask him about actual things he may have seen.

MR. DRATEL

Sure.

Q. Silk Road users, in the context of how the bitcoin server worked on Silk Road, --

A. Okay.

Q. -- Silk Road users, a purchaser of a product off of Silk Road, would have a wallet on the Silk Road server, correct?

MR. TURNER

Objection to foundation.

THE COURT

Overruled.

A. I don't believe they have a wallet, but they're given an address where they could deposit the bitcoins that they personally own.

Q. Right. And then they could withdraw those bitcoins, correct?

A. I believe so; yes.

Q. And those bitcoins being withdrawn would show up as a transaction on the block chain from the Silk Road server to one of their addresses in a bitcoin wallet, correct?

A. Can you repeat that, please.

Q. Sure. That if a Silk Road user puts --

THE COURT

Ask it in terms of what he's observed.

Q. From what you know about the operation of the server with respect to bitcoins on Silk Road, that a user would fund his address, right, on Silk Road, correct?

A. Correct.

Q. And then if they decided to withdraw those bitcoins rather than using them to purchase at some point if they had a balance left, they could withdraw those bitcoins and that would show up as a transaction on the block chain from Silk Road wallets, correct?

A. Correct.

Q. In fact, someone could use Silk Road as a wallet itself in that forum, right?

A. I guess you could, but it's kind of dangerous to trust your bitcoins in someone else's wallet management.

Q. But it could be done?

A. It could be done, but when we seize government -- when the government seized the Silk Road server, anyone who left their bitcoins in their Silk Road address for the purchase of buying drugs, they lost all their bitcoins, so I wouldn't maintain my bitcoins that way.

MR. DRATEL

One moment.

THE COURT

Yes.

Q. Now, part of your investigation, part of what you were doing is looking at the movement of bitcoins back and forth, correct, from Silk Road servers, right?

A. Not back and forth. Just one direction from Silk Road to the Ross' laptop.

Q. And you mentioned --

THE COURT

I want to make sure that you don't speak over the witness.

MR. DRATEL

I'm sorry.

Q. But you mentioned that the amount that was in the FBI wallet was actually larger than the amount that was in -- that was transferred from the laptop, right?

A. Yes. So once the transaction -- once the seizure happened, FBI address made it onto the block chain and transaction of that size normally gets noticed by a lot of bitcoin users. So once that happened, the government seizure address was publicly known at that point. And just like -- just like an email, someone could send you an email and you send end up receiving it, whether it's spam or not. So we received a lot of small transactions that also came into the government wallet -- government address.

Q. Bitcoin?

A. Small -- fractions of bitcoins.

Q. But you don't know where they were from necessarily, right, you didn't track them all down?

A. I'm sorry. What was that?

Page 1744
Q. You didn't track down where they all came from?

A. No, I did not.

Q. So when you say spam or something, that's just your speculation, right?

A. Right.

Q. That's just a theory. You don't know where those -- those bitcoins came from after Mr. Ulbricht's arrest, right?

A. Right.

Q. And in fact, when you talked about large amounts being noticed on the block chain by the public, in fact, you -- six weeks after Mr. Ulbricht was arrested, you noticed 195,000 bitcoins being moved, right?

A. 195,000 bitcoins?

Q. Yes.

A. I don't recollect that.

Q. I'll show you what's marked as 3511-38 and ask you if that refreshes your recollection. That November 22nd, 2013, there was a 195,000 bitcoin transaction that was then broken down quickly into three different transactions, right?

A. I'm sorry. I was reading this. Could you give me just one second.

Q. I'm sorry.

A. Yes. You may proceed.

Q. I'm sorry. It was 35, not 38. Thank you. It's the wrong one. I'm giving you 35 instead to read.

Page 1745
A. Sure.

Q. No wonder you're confused. Does that refresh your recollection: November 22nd, 2013, that there was a transaction of 195,000 bitcoin that that was then quickly broken up into three smaller transactions?

A. It looks familiar; yes.

Q. Now, you you're at something called FTI Consulting, right?

A. Yes.

Q. And you left the government to join that organization, right?

A. Yes.

Q. The amount of money that the company's been paid already for this work is $55,000, right?

A. We haven't been paid yet. I'm not sure what the bill is going to --

Q. Is that the bill you've run up, $55,000, right?

A. I'm not sure of the exact amount, but I think it's somewhere around there.

Q. And this was an important case, right, for you and your career?

MR. HOWARD

Objection.

THE COURT

You mean in his career with the government or at FTI?

MR. DRATEL

Well, both, your Honor.

THE COURT

All right.

Page 1746
Has it been important in your career in both jobs? You may answer.

A. It was a significant case considering that bitcoin was never involved in a criminal case like this, but I've worked on many other cases that were very interesting as well.

Q. And it's also true that another agent closely involved in this case, Christopher Tarbell, also went to FTI after the arrest in this case, correct?

A. Yes.

MR. HOWARD

Objection; beyond the scope.

THE COURT

Overruled.

MR. DRATEL

Q. The answer is yes, right?

A. Yes.

Q. And you left during this -- after the arrest and before the trial, right, and you went to FTI?

A. Yes.

MR. DRATEL

I have nothing further.

THE COURT

Thank you.