UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
Plaintiff,	)	
v.	)	Criminal Action No. 13-10200-GAO
DZHOKHAR A. TSARNAEV, also known as Jahar Tsarni,	)	
Defendant.	)	

BEFORE THE HONORABLE GEORGE A. O'TOOLE, JR.
UNITED STATES DISTRICT JUDGE

EXCERPT OF JURY TRIAL - DAY THIRTY-SEVEN

Testimony of Kevin Swindon

John J. Moakley United States Courthouse
Courtroom No. 9
One Courthouse Way
Boston, Massachusetts 02210
Monday, March 23, 2015
9:10 a.m.

Marcia G. Patrisso, RMR, CRR
Cheryl Dahlstrom, RMR, CRR
Official Court Reporters
John J. Moakley U.S. Courthouse
One Courthouse Way, Room 3510
Boston, Massachusetts 02210
(617) 737-8728

Mechanical Steno - Computer-Aided Transcript

APPEARANCES:

OFFICE OF THE UNITED STATES ATTORNEY
By: William D. Weinreb, Aloke Chakravarty and
Nadine Pellegrini, Assistant U.S. Attorneys
John Joseph Moakley Federal Courthouse
Suite 9200
Boston, Massachusetts 02210
- and -
UNITED STATES DEPARTMENT OF JUSTICE
By: Steven D. Mellin, Assistant U.S. Attorney
Capital Case Section
1331 F Street, N.W.
Washington, D.C. 20530
On Behalf of the Government

FEDERAL PUBLIC DEFENDER OFFICE
By: Miriam Conrad, William W. Fick and Timothy G.
Watkins, Federal Public Defenders
51 Sleeper Street
Fifth Floor
Boston, Massachusetts 02210
- and -
CLARKE & RICE, APC
By: Judy Clarke, Esq.
1010 Second Avenue
Suite 1800
San Diego, California 92101
- and -
LAW OFFICE OF DAVID I. BRUCK
By: David I. Bruck, Esq.
220 Sydney Lewis Hall
Lexington, Virginia 24450
On Behalf of the Defendant

I N D E X

* * * * * *

E X H I B I T S

P R O C E E D I N G S

THE COURT: Morning.

MR. CHAKRAVARTY: Your Honor, Agent Swindon is still on the stand. I have a few minutes left with him just to clarify some things, and then I would hand him over for cross-examination. My understanding there's anticipated to be a lengthy cross-examination of this witness. And the next witness is Dr. Levitt, who is our terrorism expert. He has a flight to Europe scheduled for this afternoon after the court day. And so our hope was that we would get all of his testimony in.

In light of the prospect of Mr. Swindon potentially going longer than expected, if the Court has no objection, I'd like to potentially call Mr. Levitt out of order -- Dr. Levitt out of order and then conclude Agent Swindon's.

THE COURT: Mr. Bruck?

MR. BRUCK: That's fine with us, your Honor. I should note, however, that there is a motion in limine respecting the terrorism experts, of which Dr. Levitt is one. And his report is specifically referenced in that motion. So that will have to be addressed before his testimony.

THE COURT: Well, I've reviewed his report, and I think he can testify. So as to him, it's denied. The motion is denied as to him. I've reviewed the report and the motion. The motion was addressed to a number of people, and I take no

position whether it applies to others or not -- whether this ruling applies to others or not. As to him, he may testify.

MR. BRUCK: That leaves me, I guess, with the question about the extent to which I will have to continually object during the course of his testimony on the grounds stated in the motion in limine or whether we can have a continuing objection to the background information.

THE COURT: Yes, you may have a continuing objection to it.

00:01 MR. BRUCK: Thank you very much.

THE COURT: How long will the Levitt testimony be?

MR. CHAKRAVARTY: I anticipate -- it's my anticipation so it might be generous -- about an hour and a half on direct, your Honor.

THE COURT: On direct?

MR. CHAKRAVARTY: On direct.

THE COURT: And how much on cross?

MR. BRUCK: Considerably less than that, your Honor.

THE COURT: Well -- so who's doing the cross of this

00:02 witness?

MR. FICK: I am, your Honor.

THE COURT: And your estimate?

MR. FICK: Possibly a couple of hours.

THE COURT: Yeah. Well, why don't we proceed -- well, there's two ways of doing it, I guess. You can finish the

direct, and we can go to Levitt and get him done and then have the cross uninterrupted, or you can have some cross and we'll see how the clock goes.

MR. BRUCK: As far as Levitt goes, I don't think there's any danger, that if we proceed in the normal order, that he wouldn't be finished by 4:00 at least based on --

THE COURT: Okay. All right. Let's see how the morning goes then in the normal order.

MR. FICK: So we can proceed --

00:02 THE COURT: So you'll begin with cross after the direct; is that all right?

MR. FICK: Yeah. I'm going to have my consultant come to the table.

THE COURT: Fine. Any other issues before we get the jury? So why don't you line them up. It takes awhile usually.

Miss Conrad filed a motion under seal this morning.

MS. CONRAD: Yes, your Honor.

THE COURT: That matter has to be addressed to the presiding judge in the other case.

00:03 MS. CONRAD: Okay. Thank you.

THE COURT: As a preliminary matter.

MS. CONRAD: Okay. Thank you.

THE COURT: It may then be appropriate depending on the ruling, okay?

MS. CONRAD: Yes.

(The jury entered the courtroom at 9:13 a.m.)

THE COURT: Morning, jurors. I hope you had a good weekend, and I hope you abided by my instructions not to discuss the case. Did you?

THE JURY: Yes.

THE COURT: Thank you. We'll resume with the direct examination of Agent Swindon.

MR. CHAKRAVARTY: Thank you, your Honor.

CONTINUED DIRECT EXAMINATION BY MR. CHAKRAVARTY:

00:04 Q. Good morning, Agent Swindon.

A. Good morning.

Q. I just wanted to clarify a few things before I hand you over for cross-examination.

We had talked on Thursday about some of the items that you had found on the Sony VAIO laptop, what you called the 1R6, Exhibit 1142. Do you remember that?

A. Yes.

Q. Was one of those items a folder that was marked as a Mobilsync backup?

00:04 A. There was a file named Mobilsync backup.

Q. Can you just explain again what that was?

A. The Mobilsync backup is a backup of the iPhone or an Apple device that would be stored on the computer if you backed it up.

Q. And what kinds of data were stored in the Mobilsync

backup?
A. The Mobilsync backup has a standard set of things it attempts to try and store but not always successful. Typically it would be contacts, text messages, the actual ID of the phone, of the SIM card ID on the phone, and maybe images and other data that would be on the phone.
Q. And so on the -- on that device, did you locate several text messages that were then exported and you verified that those did appear, in fact, on the Sony VAIO computer?
00:05 A. The text messages were in the Mobilsync backup data that was exported.
Q. Specifically, were there Exhibits No. 1385 through 1389, 1393, and 1395? Would it help to put them up on the screen?
A. It would, yes.
MR. CHAKRAVARTY: Your Honor, for the witness, please.
Q. So this is 1385, 1386, 1387, 1388, 1389, 1393, and 1395. Do you recognize those as being text messages that were exported from the Sony VAIO laptop along with a redaction of the identifying information of the counterparty to a
00:07 conversation?
A. Yes. Those messages were located in Mobilsync backup data from the 1R6.
MR. CHAKRAVARTY: I'd move into evidence 1385 through 1389, 1393, and 1395.
MR. FICK: Same objection to the extent these are

derivatives compiled by somebody else.

THE COURT: All right. Overruled. Admitted.

(Government Exhibit Nos. 1385-1389, 1393, 1395 received into evidence.)

Q. With regards to this Mobilsync backup, I had asked you a little bit on Thursday with regards to whether you were able to identify which phone actually produced those text messages. I should say which phone had synced with the laptop that resulted in those text messages going over to the laptop. Were you able to determine that?

A. Yes. With the exception of 1385, the messages were included in the iPhone 5 backup.

Q. I'm sorry. 1385, was that a different iPhone?

A. Yes. That came from the iPhone 3. That was another Mobilsync backup that was on the device.

Q. Thank you for clarifying that.

For the remainder, which phone were you able to attribute those to?

A. All but 1385?

Q. All but 1385.

A. Yes. The iPhone 5.

Q. And that's --

MR. CHAKRAVARTY: I think this is in evidence. Your Honor, if I could have this published?

THE COURT: Displayed?

MR. CHAKRAVARTY: Yes, please.

Q. This is what's marked 1411, also on the 1R6 device. Was there an ICC ID number on this?

A. Yes.

Q. Were you able to match that up with an ICC ID number somewhere else in the investigation?

A. Yes, from the iPhone 5 on -- I believe it's 2W1.

Q. Moving over to --

A. I'm sorry.

00:09 Q. 2W2?

A. 2W2, I'm sorry.

Q. Were you able to read the SIM card, and is that the same number?

A. Yes.

Q. I just pulled up on the screen 1151-16, which is a photograph of the SIM card that you looked at on Thursday, is that right?

A. Yes.

Q. In addition, I had asked you on Thursday whether there

00:09 were some text messages that were extracted from an iPhone of Dias Kadyrbayev. Do you recall that?

A. I do, yes.

Q. Over the weekend, were we able to redact a version of those text messages?

A. Yes.

MR. CHAKRAVARTY: And I'd move into evidence Exhibit 1153, which is the redacted version.

MR. FICK: Still the confrontation and foundation objection.

THE COURT: All right. Subject to that objection, overruled. Admitted.

(Exhibit No. 1153 received into evidence.)

MR. CHAKRAVARTY: Call up 1153 on Sanction, please.

THE COURT: Publish?

00:10 MR. CHAKRAVARTY: Yes, please. Thank you.

Q. Agent Swindon, are these text messages that were from April 18, 2013, from Dias Kadyrbayev's phone between Dias and the person listed as Jahar, with a phone number 857-247-5112?

A. These messages were present on that phone, yes.

Q. The text box on the right, does it say, "I saw the news"? "Better not text me, my friend." And then --

A. Yes.

Q. And then does that same user say, "If you want, you can go to my room and take what's there, Smiley face, Bro, salaam

00:11 alaikum"?

A. Yes.

Q. Now, I wanted to clarify --

MR. CHAKRAVARTY: Thank you, Mr. Bruemmer.

Q. I wanted to clarify a few points about a couple of the devices, the external hard drive devices. There was one that

was found in Watertown, on Laurel Street, that we've introduced as Exhibit 1475. Do you recall that?
A. Yes. Can you bring up the original exhibit that had the list, please?
Q. Sure. You want the list, the spreadsheet?
A. Yes, please.
Q. So we were talking about the 1W16, is that right?
A. Yes, sir.
Q. And were there certain files that were -- appeared to be
00:12 scanned versions of Russian textbooks on this hard drive?
A. There were files on that 1W16 that were in a format -- that were recovered in a format called DjVu. DjVu is a proprietary format, similar to, like, a PDF file or an Adobe PDF, although not widely used anymore. Those files were converted from DjVu to PDFs for trial purposes or exhibit purposes.
Q. And so moving into that hard drive, is this an example of the fact that those are now PDFs so that they can be opened in front of the jury?
00:13 A. Yes.
Q. On that same hard drive, I think you mentioned on Thursday that there was a file that appeared to be a document which was a homework assignment of somebody that -- named Giovanni Norgill. Was that in the active directory of the computer hard drive, or where did you locate that?

A. Could you go back one, please?
Q. Sure.
A. Thank you. Yeah, the 1475-03 was a carved/recovered file from a previous directory structure that existed on the hard drive.
MR. FICK: Your Honor, I'd just ask the exhibit be modified at a convenient time to conform to the format of the other exhibits where carved files were stored separately so as not to mislead anybody.
00:14 THE COURT: I'm not sure I followed that. They're organized --
MR. FICK: The exhibits have largely been organized to sort of show the location of the files the way they were on the active device. Where there were carved files on most of the other exhibits, those were put in a separate folder so no one is confused about whether they were there or whether they were deleted and recovered.
MR. CHAKRAVARTY: I don't have a problem with that, your Honor.
00:14 THE COURT: Okay.
Q. Now, these DjVu files -- DjVu is just a -- is that a software tool?
A. It's a file format that they would be put into.
Q. Were there also DjVu files found on the thumb drive that was found in the landfill that you've called L14 and we've

marked as 1150?
A. Could you go back to the spreadsheet, please? Yes.
Q. And with regards to those DjVu files, were those also converted to PDF?
A. Those were also converted to PDF.
Q. Were some of those DjVu files actually corrupted, and you weren't able to access them?
A. I believe that four of those files were corrupted and unable to be accessed.
00:15 Q. To refresh your memory, was it Files No. 26, 27, 28, and 33 that were corrupted?
A. Yes, it was.
Q. For purposes of trial presentation, were those replaced with intact versions of those PDFs from another device?
A. The disks that I was asked to review had an intact version of that file on it.
Q. But it wasn't intact when you found it?
A. It was not.
MR. FICK: Again, I'd ask the exhibit then be modified
00:15 to conform to what was actually there.
MR. CHAKRAVARTY: Again, no objection, your Honor.
THE COURT: Okay.
Q. Now, the names of carved files, you explained what carving is. I'm not going to ask you to rehash what that is. But what did the names of carved files appear as when they're carved out

of this unallocated space?
A. In the application software, it doesn't -- it's not coming out of a directory so it doesn't have the name of the file, although it might be able to carve that file out of the unallocated space. It has to find some way of accessing it in the application software. So it starts a numerical numbering system unique to that carved file.
Q. What is the name when your software exports a carved -- a series of 1's and 0's that software recognizes to be a file, what does it name that file?
00:16
A. It would be a sequential number that was generated by the application software.
Q. Again, for trial presentation purposes, where there was no name on the file itself, or no decipherable name on the file itself, but there was in the document, were any of the documents' titles changed in order to reflect the content?
A. The carved file titles were changed to reflect the content, yes.
MR. FICK: Same request to correct the exhibit.
00:17
THE COURT: Okay. All right.
Q. Now, sticking with this thumb drive that was found in the landfill, were you able to determine whether that thumb drive had ever been plugged into the Sony VAIO laptop computer, 1R6, Exhibit 1142?
A. Yes, we were.

Q. How were you able to do that?
A. Again, from Thursday, the registry file which is associated with every Windows computer collects and stores information of devices that were installed into that -- into that computer. And there was an entry in that registry that showed the serial number from that thumb drive in the registry file.
Q. If I may ask to publish Exhibit 1142-02, does this show a Kingston thumb drive being plugged into the 1R6 computer from the registry information?
A. This information was extracted from a link file, and it shows the volume serial number which is unique to the Kingston thumb drive -- or this particular Kingston thumb drive.
Q. You checked the registry to match up that Kingston thumb drive to the one that was found in the landfill?
A. Yes.
Q. We had talked a little bit about Tamerlan's computer, the D385 that was found in Laurel Street in Watertown; do you remember that?
A. We did, yes.
Q. You didn't do the same extraction of files or verification of files that were on that computer, did you?
A. We did not.
Q. Did you find files of a similar nature on that computer as those that you talked about?

A. There was a cursory look of that computer done, and there were numerous files that were of the same title.
Q. Was there anything unique about how Tamerlan's computer was set up?
A. One unique thing is that on D385 had a TrueCrypt volume on the drive. And TrueCrypt is an encryption software. It's readily available and it's actually freeware. You can download, and it will allow you to be able to encrypt a file, a folder or a drive -- or a volume, I'm sorry.
00:19 Q. When you say "encrypt," what does that mean generally?
A. Encrypt would be to change it from cleartext, which is readable, to a ciphertext, which would be unreadable to anybody who didn't have the password to decrypt it.
Q. That's another type of password protection?
A. It would be more data protection than password protection.
Q. Finally, I asked you about some of the commonalities of files across some of the devices on Thursday.
MR. CHAKRAVARTY: Can we call up Exhibit 1438 just for the witness?
00:20 Q. Do you recognize this chart?
A. I do, yes.
Q. What is it?
A. This is an MD5 hash analysis, as we talked about on Thursday, which is the sort of fingerprint for the file. And this is an analysis of files that are common across 1R6, 1437,

14-6, and 3R5.
Q. So those are four devices that you talked about on Thursday?
A. Yes.
Q. And would this chart help you explain some of the propagation of those files across those devices to the jury?
MR. FICK: Objection to the form of the question.
THE COURT: Overruled. You may answer.
A. Yes.
00:21 MR. CHAKRAVARTY: Your Honor, I'd mark this as a chalk, please, and ask to publish.
THE COURT: Okay.
Q. Agent Swindon, is this a selected file listing from the 1R6 Sony VAIO laptop, 1142?
A. Yes, it is.
Q. And are these some of the audio files from that computer that we can see from the MP3 file type?
A. Yes.
Q. Did you see these across various devices?
00:21 A. We did.
Q. Moving on in the same chart, did you see the same files on the iPod Nano labeled "Jahar"?
A. Yes.
Q. How did you determine that they were the same files?
A. Not only do the -- in most cases, the title of the files

match but the MD5 hash value matches.
Q. And the MD5 hash value you described as the fingerprint for each file?
A. Yes.
Q. And did you find the same files on the iPod Shuffle that was found in Watertown that was labeled "MP3 play"?
A. Yes.
Q. Again, was it through the same MD5 hash value analysis?
A. Yes.
00:22 Q. And the 3R5, which was the Samsung Finesse phone that was found in the dormitory room at UMass Dartmouth, did you find those same files?
A. Yes.
Q. And so does this table indicate the common files that -- those common files that you just mentioned that were on all four of those devices?
A. Those particular files, yes.
MR. CHAKRAVARTY: Your Honor, I think foundation has been met to move to introduce this as evidence under 1006, your
00:23 Honor, so I would so move.
MR. FICK: I'd object to the word -- the title of the file because it suggests a direction of the movement has not been established.
THE COURT: Overruled. I'll admit it as an exhibit. What's its number?

MR. CHAKRAVARTY: 1438.

THE COURT: Okay.

(Exhibit No. 1438 received into evidence.)

MR. CHAKRAVARTY: Those are all the questions I have for Agent Swindon at this time, your Honor.

MR. FICK: Just a moment to set up.

CROSS-EXAMINATION BY MR. FICK:

Q. Good morning, Agent Swindon.

A. Good morning.

00:24 Q. My name is Bill Fick. I'm one of Mr. Tsarnaev's attorneys.

You spent a good part of your testimony, both today and last week, talking about Exhibit 1142, which are the collection of files from the Sony VAIO, right?

A. Yes.

Q. And at one point last week when you were talking about that exhibit, you said -- and I think -- I'm quoting, "This was a representative sample that was given to us to verify." Do you remember saying that?

00:25 A. Yes.

Q. And that actually wasn't an accurate statement, right, because there's nothing representative at all about what's on 1142, fair to say?

A. That was a sample of what was on 1142.

Q. A sample selected by the investigative team at the FBI,

right?
A. By the investigative team.
Q. So it's not representative in some proportional way of what was on the Sony, right?
A. There were hundreds of thousands of files on the Sony 1R6.
Q. Just to make it a little more concrete, there was a lot of Mr. Tsarnaev's homework on the Sony, right?
A. I would have to confirm it by looking at it, but I wasn't asked to verify that there was particular homework assignments
00:25 on it.
Q. There was one homework assignment among the exhibits that you talked about, right? And that was an assignment about drones from high school; do you remember that?
A. If you could pull it up for me, sure.
Q. Just to go backwards, you recognize this as being Exhibit 1142, right? Going inside the Sony laptop, going to public, and the first document there is the assignment about drones that I believe you talked about, is that right?
A. I verified that 147 existed on that computer, yes.
00:26 Q. You're aware that there were other homework assignments on the computer right? You looked at the computer, and this was one file that was selected for you to make sure was there?
A. There was numerous documents and files on that computer.
Q. And the Exhibit 1142 that you talked about also included a selection of audio files, music, right? The nasheeds we've

been talking about that you verified?
A. Yeah. There were nasheed files on that computer, yes.
Q. That was a selection that the investigative team gave you that you then verified were there, right?
A. Yes.
Q. And we're talking about -- it was a couple dozen files, something like that, that you talked about?
A. I'd have to see the exact number, but I don't have that in front of me.
00:27 Q. All right. Well, we can do that again.
THE COURT: Mr. Fick, I'm not clear whether you want this just for the witness or for the witness and the jury.
MR. FICK: I'm going through stuff that's in evidence, your Honor, so I would leave it on the screen if that's okay.
THE COURT: Okay.
MR. FICK: Thank you.
Q. Well, whatever the number was, the bottom line is there was a group of files that were on the disk that we talked about -- that you talked about last week that you verified, right?
00:28 A. There were files that I was asked to verify existed on that commuter, yes.
Q. And it was a small collection of the over 400 MP3 audio files that were on that computer, right?
A. I don't know the exact number of MP3 files on the computer.

Q. When you were in the process of verifying the files, you looked at the 4,000-or-so-page long list of everything on the computer, right?
A. We did a comparison, yes.
Q. So you have noticed, in looking at that list, there were many hundreds of audio files on the computer, correct?
A. Again, I don't know how many MP3 files were on that computer in total.
Q. Are you willing to even estimate that we're talking many
00:29 hundreds of files?
A. Not without the time to be able to analyze the data.
Q. Well, in any event, in addition to the nasheeds that you talked about in your testimony --
MR. FICK: If I can get my screen back here.
Q. -- there were -- there was pop music on the computer, right? Did you happen to notice that when you were looking at the audio files?
A. I would only recognize them by the titles of the MP3s when I was looking through and verifying the ones I was asked to
00:30 verify. I did not listen to the actual MP3 files. We weren't asked to verify.
Q. Fair to say you recognized a large number of pop music audio titles in verifying the MP3 files on the computer, correct?
A. There were a few titles there that I would recognize, yes.

Q. Just by way of example, I'm going to pull up a screenshot of Page 2126 of Exhibit 1142-152. And, for example, the title we've heard other times in this trial is on this computer, Jay-Z, *Ain't No Love in the Heart of the City*; do you see that?
A. I do see that. 1142, is that the actual exhibit that I'm looking at?
Q. Yes. You're looking at Page 2126 from Exhibit 1142-151. Do you see that?
A. If that's the complete file listing from 1142, then, yes.
00:30 Q. And that's the complete file listing or something like it that you used to go through and verify whether various files were on the computer, correct?
A. That is one of the techniques that we used, yes.
Q. And the total number of exhibits -- sub-exhibits numbered on 1142, I think the highest number is 151 or something like that, is that right?
A. I would have to see it, sir.
Q. Okay. We'll pull it up again. 1142-151, that's the sort of last document there. That's the giant file listing we were
00:31 just looking at, right?
A. I believe that's the last file -- the last exhibit from that piece of evidence, yes.
Q. 151 sub-exhibits from this computer out of a half a million files, is that right?
A. That would be fair to say, yes.

Q. So we're talking about something like three-ten-thousandths of one percent of the files from that computer, right?
A. I don't think it's realistic that we looked at every single solitary file on that computer to show here in court.
Q. I'm not asking you if you looked at every single solitary file. I'm just asking whether the selection that the investigative team included on this disk is a flyspeck compared to 500,000?
00:32 A. I'm not sure what the definition of a flyspeck is, but if you'd want to go back to the percentage, we could do the math, I guess.
Q. Who selected what files were going to go on this disk? You said it wasn't you.
A. There was an investigative team which was made up of investigative analysts, case agents, prosecutors, forensic specialists. And that's primarily members of the investigative team.
Q. Can we put some names on that? Do you know who actually
00:32 made the choice?
MR. CHAKRAVARTY: Objection, your Honor. It's asking him to speculate.
THE COURT: No. You may answer if you know.
A. I don't know who actually selected every single individual one of these files. I do not.

Q. So do you believe it was different people that did it, multiple people that did it?
A. There were multiple analysts that were working on this investigation, yes.
Q. Who sort of provided you with the finished package? Who tasked you with, Here's a list? Check and see if they are there?
A. That was a combination of the senior investigative analyst, the case agents, and the prosecutors.
00:33 Q. So who's the senior investigative analyst?
A. John Petrozelli.
Q. And him and a collection of case agents and the prosecutors together, in some ceremonial forum, gave you the disks altogether?
A. Well, it wasn't very ceremonious. It was, Here's a stack of CDs, and I need you to verify and validate that there's information on these CDs.
Q. Bottom line is you're not the one who selected them?
A. I did not select them, no.
00:33 Q. Okay. Now, what about the various spreadsheets that are in each of these exhibit files, the various -- these derivative exhibits you talked about, the spreadsheets of internet history selections, et cetera? Who made those?
A. The investigative team also made those.
Q. So as to any individual spreadsheet, can you say who in

particular actually made it?
A. Not every single one, no.
Q. For any of them, do you know who made them?
A. I do, yes; several, I do.
Q. For example, can you just tell me one of the ones on the screen here and tell --
A. If you'd like to pick one, I could certainly --
Q. Yes, please.
A. Which number?
00:34 Q. Well, no. You said you only knew some of them. So pick one that you know who made it and tell me.
A. Could you make the screen a little bigger, please, so I can see the complete names of the file list?
So the selected internet -- the selected internet activity or 001.
Q. Yes.
A. Yes, sir.
Q. Who made that one then?
A. That was John Petrozelli.
00:34 Q. When you went through to verify the materials on these disks, did you verify each of the spreadsheets for accuracy as well?
A. I went over the spreadsheets with Mr. Petrozelli, and we accessed the Internet Evidence Finder data and compared the two, yes.

Q. So did you compare them line by line?
A. We went line by line with the results from his Internet Evidence Finder search.
Q. Now, what about exhibits that aren't from internet evidence, exhibits that are fileless from the computer, did you verify those line by line?
A. The file list for the computers are generated by the forensic software, which they're approved tools. Previous to us using the tool, that file listing is an accepted practice
00:35 within the SOPs of the guidelines.
Q. I understand, for example, that -- correct me if I'm wrong -- something like Exhibit 151, the massive 4,000-page list, that's generated by a computer or software, right?
A. That's generated -- actually, the name is in the title. It's generated by a product called X-Ways Forensics.
Q. But the other exhibits, the sort of subsets, the derivative samples, the extractions of a limited number of files, that's done by some human being, right? If you just take, for example -- let me just ask the question more
00:36 generally. There's the 4,000-page list of all the files in the computer, right?
A. Yes, sir.
Q. There were various other spreadsheets with lesser lists of certain files that the FBI determined were relevant to the investigation you should talk about, right?

A. You mean lesser directory listing files?
Q. Lists, sublists of the big one. They contain a smaller number of files in the list.
A. There are derivative lists that have been entered in as evidence that were sublists of other information or have been gotten from the computer.
Q. For example, 1142-13, right, these are various selected user files from the Sony laptop, right?
A. Yes.
00:37 Q. And this is a five-page spreadsheet as opposed to 4,000 pages, right?
A. Yes.
Q. So some human being picked some of the files on the 4,000-page list and included them on the smaller five-page list, right?
A. Yes.
Q. Okay. As to such spreadsheets, the smaller lists, the sublists, did you go through each of those and verify that each of the actual entries, the files and the dates and times
00:37 associated with them, were actually on the master list?
A. These were generated from the master list.
Q. They were generated from the master list in the form of somebody cuts and pastes different entries, right?
A. Again, I'm not sure the process, whether they were hand-typed or cut and pasted, but these were generated from

information that was from the main directory listing in the case.

Q. Okay. Did you go through them line by line and make sure there was no error in the moving from here to there, as a general matter, for all of these spreadsheets?

A. Well, I verified that the information included in these spreadsheets is included in the master directory listing.

Q. My question is a little bit different. I'm talking about did you go through line by line and make sure nothing

00:38 extraneous got in there, nothing fell out that should be there?

A. I verified that the information that is in the spreadsheets that were generated from the master directory list was in the master directory list.

Q. Did you do that on a line-by-line basis?

A. For each of these?

Q. For each of the spreadsheets that you've talked about here.

A. Yes.

Q. Every single one?

00:38 A. Every single one, from every single piece of evidence or every single one from 1150 -- I mean 1142?

Q. Speaking generally now about the collection of exhibits that was put into evidence through you last week, each of those disks has a number of derivative spreadsheets on them, fair to say?

A. They have a number of different types of spreadsheets, yes.
Q. Among those spreadsheets on each of them is a derivative spreadsheet, a selected file list from each of the devices, right?
A. Not every single one.
Q. Let me try and ask the question a little bit more specifically then. As to Exhibit 1142-13, the selected file list off of the Sony, did you review that spreadsheet line by line to make sure it was all accurate?
00:39
A. I did.
Q. Okay. And did you do the same thing for all of the other like spreadsheets that are derivative file lists in the other exhibits?
A. Right. But there are a number of different types of spreadsheets that are in each of the different types of evidence, so there may have been different techniques used.
Q. Okay. As a general matter, for whatever the technique was, did you verify each spreadsheet line by line?
00:39
A. Not general but specifically, yes.
Q. Now, you are a supervisory special agent, right?
A. I am, yes.
Q. And you're both an agent and a certified computer analyst, right?
A. Certified computer analyst? I'm not sure what that means.

Q. Well, you talked about the various kinds of training and certification you have in computer forensics, right?
A. Prior to being a supervisor, I was a certified forensic examiner, yes.
Q. And so you have training as both sort of the standard FBI agent training, and you have additional specializations in computer forensics, fair to say?
A. Yes.
Q. And you are the supervisor in Boston for both the Cyber
00:40 National Security Squad and for the CART team; as I understood it, correct?
A. Yes. The CART program comes under my supervision.
Q. And remind us again what CART stands for.
A. It's the Computer Analysis Response Team.
Q. And so the people you supervised did a lot of work collecting, processing and analyzing the hundreds of pieces of digital evidence that were collected in this case, right?
A. Yeah, people that I directly supervise and then people from other field offices also, yes.
00:40 Q. But you are the CART supervisor in Boston, right?
A. I am the supervisor for the CART program in Boston, yes.
Q. And the various items, if we pull up, for example, the little exhibit, the chalk, that Mr. Chakravarty talked about with you a fair amount -- I believe it was marked as 1557. In general, the items that you've been talking about were all

processed at either Black Falcon or Center Plaza here, right?
A. Or Quantico, yes.
Q. Or Quantico, a few of them down at the bottom. But a large number of them at Black Falcon and Quantico, right?
A. Center --
Q. I'm sorry, Black Falcon and Center Plaza, right?
A. Yes.
Q. Those are the -- these -- that's where the CART people worked that you supervise, right?
00:41 A. Not permanently. They work in Center Plaza. Black Falcon was the --
Q. It was temporary?
A. Yes.
Q. But you supervise CART in Boston; that's the bottom line?
A. Yes.
Q. Now, so you then had an oversight role in the activities of analyzing the data from the devices collected in the Boston Marathon investigation, right?
A. A -- I had an oversight role of the individuals or the
00:42 people that were responsible, yes.
Q. As time went on, as a supervisor, you reviewed their work product from time to time, right?
A. We do periodic file reviews of what's assigned to individual examiners, but I don't micro what they're working on in any one given time.

Q. But you're certainly aware of what the people under your supervision are doing, right?
A. Yes.
Q. And you discuss issues that may come up from time to time, right?
A. Technical issues or personnel issues?
Q. Issues related to the work that they are doing on the investigation.
A. Yes.
00:42 Q. So you have an awareness of the investigation of digital evidence related to the Boston Marathon bombing?
A. Yes.
Q. Pretty big investigation in your career, I take it, right, in terms of scope and complexity?
A. One of them, yes. I mean, it's not -- it's the same proportion as 911 or several others that I've been involved in, yes.
Q. Big, big operation?
A. Yes.
00:43 Q. I think you testified that the FBI has a very standardized process for acquiring and processing digital evidence, right?
A. The certification process has -- yes, has -- to become a certified examiner, there is a standard process, yes.
Q. The process of actually doing the investigation, taking the device, imaging it, processing it, that's all very

standardized also, isn't it?
A. Yes.
Q. It's important to document that process, too, at each step of the way, to record what has happened and who did it, right?
A. It's different for different devices, and each examiner is -- has their sort of own way of doing it.
Q. Well, there's a standard chain of custody, for example, that the FBI maintains for electronic evidence in these kinds of investigations, right?
00:44 A. Yes.
Q. So that keeps track of a device gets imaged, right? That's part of what happens here. There's a recording of the fact of the device being imaged, right?
A. Well, the chain of custody is for the handling of evidence, not --
Q. Right.
A. Not the process of the imaging or the processing.
Q. When a piece of evidence comes in and is imaged, that fact is recorded as part of the chain of custody, right?
00:44 A. No.
Q. It's not?
A. It is not.
Q. Is there any other form in which the various steps taken by the various people along the way in processing a piece of digital evidence are recorded?

A. It would be in a final report.
Q. So there's no sort of ongoing, something -- there's nothing analogous to a chain of custody for each step in the process for a forensic investigation?
A. There is not, no.
Q. So, for example, going back now, we couldn't retrace the steps of who did what from the moment of collecting the Sony laptop through the present? We couldn't retrace that in a paper trail?
00:45 A. Well, we could, sure.
Q. Using what then if there's no chain of custody that records that?
A. There's the chain of custody for the actual piece of evidence. We could show you who had custody of that piece of evidence. Then, typically, in the notes that you'll see -- that we saw that we included in 1R6, you can see the name of the person who would have imaged it.
Q. What about somebody who then processed the image, is that recorded somewhere?
00:45 A. That would be in a final 302 report or a final report, yes.
Q. So is it standard then for there to be some kind of a final 302 report or other report about the analysis of a piece of digital evidence?
A. At the conclusion of the request from the case agent or

from an analyst, the CART examiner would do a final sort of piece of paper -- a final, I guess you would say, report of what the activities that took place during the --

Q. A narrative report describing the examination of a device is typically produced at the end of the road?

A. It would be more technical. It would be very technical, but, yes.

Q. I'm going to show you a document and see if you recognize it.

00:46 MR. FICK: May I approach, your Honor?

THE COURT: You may.

Q. Take a quick look at that, and tell me if you're familiar with that document or you recognize what it is.

You recognize that document?

A. I recognize that document.

Q. It's a document you've seen before?

A. I have, yes.

Q. Is that something that you were involved in helping to prepare?

00:47 A. No.

Q. Do people you supervise -- were people you supervised involved in helping to prepare that?

A. One of the names on the report is somebody I do supervise, yes.

Q. Who is that?

A. Nathans.
Q. Were you aware of the work being done on an ongoing basis as that report was being put together?
A. Again, I'm not from a micromanagement standard. I do know that Nick Nathans was assigned with Petrozelli, and they were working on scoping down the voluminous information from the investigation.
Q. Okay. So the report is 53 pages long, right?
A. I have 53 pages, yup.
00:48 Q. And this is -- it's essentially a report of examination by FBI personnel about their review of the Sony VAIO, right?
A. I would say it's more of an analytical product than it is an examination product.
Q. Well, it's a report of what the examiners found in looking at the Sony VAIO, right?
A. I believe, in the context of the way the report is written, it's an analytical product that was worked on with the forensic examiner.
Q. Now, you see at the end -- actually, before the
00:48 appendices, there's a line that says --
MR. CHAKRAVARTY: Objection to reading from this report, your Honor.
MR. FICK: Well.
Q. This is not a final report, fair to say?
A. This is an analytical report. I'm not sure what you mean

by "final" or "not final."
Q. Well, toward the end it says, "Analysis remains ongoing," right?
A. Where does it say that, sir?
Q. If we could turn to Page --
MR. CHAKRAVARTY: Again, your Honor, I'm not sure this is impeachment as opposed to just trying to testify to the contents of the report that he's seen.
THE COURT: Well, go ahead.
00:49 MR. FICK: Thank you.
Q. Very last page, actually, 53.
A. Okay.
Q. Last sentence, "Digital forensic analysis remains ongoing"?
A. Yes.
Q. Do you know if there was a later iteration of this, a further iteration of something like this, an update to it?
A. I don't know what version that I have here in front of me, but I did not see an additional version.
00:49 Q. You're not aware of any additional version?
A. I'm not aware of any additional version.
Q. This version is undated, by the way, right?
A. The copy that you have is, yes.
Q. And do you know whether similar types of reports were written about any of the other devices seized in the case?

A. There were a number of 302s that were produced by numerous examiners regarding the different pieces of evidence.
Q. So there were narrative reports describing the findings of the examiners, right, for other pieces of evidence?
MR. CHAKRAVARTY: Objection, your Honor.
THE COURT: Overruled. You may answer it.
A. This report is unique in that it is a -- it's an analytical report that was worked on with the senior analyst and the CART examiner. The other reports that I'm making reference to were -- would have been final 302 reports or final reports that were technical details of what was performed during the examination, not an analytical product.
Q. So the Sony was treated uniquely? It wasn't treated the same as like the Samsung or the HP computers?
A. No. I think they were all treated the same. I think it probably garnered the most attention.
Q. Do you know whether analytic reports were produced as to the HP or the Sony?
A. Say that again.
Q. Do you know whether analytical reports were produced as to the HP or the Sony?
A. Which numbers specifically are those, sir?
Q. Going to your chart on your screen, the HP is 2R14 from Norfolk Street, and the Samsung is the 1W3 from Watertown, right?

A. Yeah. I don't recall whether or not there were reports done on those two.
Q. You don't know?
A. I don't recall.
Q. Anyway, these are the kinds of reports -- or this report of the Sony is the kind of report that FBI agents and analysts rely upon in the process of doing their investigations, correct?
A. I'm not sure what you mean by that question, but I know
00:51 this report was produced by the senior analyst that was assigned to the case.
Q. It's produced by the senior analyst and then provided to people like investigating agents and prosecutors, right?
A. It's provided to the team members, yes.
Q. And the purpose is to give them some insight into what's on that digital device, right?
A. Give them some insight or -- because, again, the volume of data is so voluminous that they need some way to be able to scope down what's on there to what's relevant to the
00:52 investigation.
Q. So this is a standard part of your practice, is to create an analytical report and provide it to the people who need it, right?
A. It's not a standard part of the process.
Q. So, again, the Sony was somehow treated differently?

A. No. I don't supervise the analytical branch, so I'm not sure what is standard practice for analytical products. I know the forensic -- the computer forensic side.

Q. Now, looking again at the chart on the screen, you testified last week and introduced a bunch of exhibits related to each of these devices, right?

A. Not all of them but some of them, yes.

Q. Do you know if the FBI has analyzed the interrelationships between these devices themselves and between these devices and

00:52 other devices?

A. There's been some analysis for that, yes.

Q. Do you know if there's been analysis of whether files, for example, can be traced moving from one to another?

A. There's been -- yes.

Q. Do you know whether there's analysis of whether these devices were connected to each other at specific times?

A. "Connected" meaning networked?

Q. Attached.

A. Attached? I don't recall whether or not there's been

00:53 analysis of whether they were actually attached. Are you talking about specifically the computers or you mean, like, a thumb drive put into a computer?

Q. For example, a few minutes ago with Mr. Chakravarty you talked about a single event where you looked at the registry and found that the Kingston was plugged into the Sony at a

certain time, right?
A. Yes.
Q. Do you know whether's there's been sort of more symptomatic investigation tracing the history of a thumb drive among all the devices in the case?
A. Among all of the computers in the case?
Q. Sure. Let's start with that.
A. So 1R6, 2R14, and D385?
Q. Right.
00:53 A. Yes. I don't recall there's been an encompassing report. I do know that we've looked at whether or not what devices had gone into 1R6 and 2R14.
Q. So 1R6 is the Sony, and 2R14 is the Hewlett-Packard from Norfolk Street, right?
A. It is, yes.
Q. Do you know if there's been similar analysis of tracing of various devices to the Samsung, 1W3?
A. D385?
Q. Yes.
00:54 A. Again, I did a cursory look of D385. I didn't do an exhaustive search or weren't asked to verify whether or not those devices were in D385.
Q. I'm not asking about your search of 385 yourself. I'm asking whether you are aware of whether the FBI did an investigation of the history of device attachments into D385 .

A. I don't recall -- I haven't seen an analytical report, so I can't comment on that.
Q. You don't know?
A. I cannot comment on that.
Q. It is fair to say you would agree with me, wouldn't you, that the interrelationship among devices can be an important thing to know in an investigation, right?
A. The interrelationship between the different pieces of evidence, say, thumb drives and computers?
00:54 Q. Yes.
A. And external drives?
Q. Yes.
A. Yes.
Q. That can tell you something about, for example, the interrelationship among suspects, among other things, right?
A. I think, like we said -- we had mentioned on Thursday, barring having a camera over somebody's shoulder, I'm not sure you could tell exactly who might be at the keyboard.
Q. But it's useful to know when various devices might have
00:55 been connected to each other and interacted with each other, right?
A. It is, yes.
Q. That can give you some evidence to make inferences about the relationships among the people who may have used those devices, right?

A. Probably more pattern-of-life information than inferences.
Q. You would also agree with me, wouldn't you, that there were other devices that were important to the Boston Marathon investigation that are not listed here at all?
A. There are over 600 -- 600 pieces of digital media alone.
Q. You have some knowledge, though, certainly of what the investigation found and how it happened, right?
A. I do in the first couple of weeks as I was intimately involved in the operations of the command post. When I assumed my regular duties, I was overseeing the computer forensic portion or the digital media portion.
Q. Right. So you supervised the CART team, the people that are analyzing these devices, right?
A. Yeah. They're providing support to the analysts, yes.
Q. Along the way then, you have knowledge of the kinds of things the people that work under you are discovering, correct?
A. In general, yes.
Q. You're aware, for example, that there were a couple computers seized also from Katherine Tsarnaeva, Tamerlan's wife, correct?
A. I would have to see the full evidence list. I don't have that list in front of me. Again, with over 600 pieces of evidence, I don't have the recollection.
Q. It doesn't stick out in your mind whether or not a couple of devices were seized from Tamerlan's wife?

A. I didn't memorize every single piece of evidence that was collected in this matter.
Q. I'm not asking that question. That wasn't my question, sir. My question was whether you have a memory or whether you have knowledge that computers were seized from Tamerlan Tsarnaev's wife.
A. Specifically from his wife or from the Norfolk location?
Q. Whether you have knowledge that computers attributed to Tamerlan Tsarnaev's wife were seized in the investigation?
00:57 A. I don't recall.
Q. You don't recall. Are you aware that cell phones attributed to Tamerlan Tsarnaev were seized in the investigation on Laurel Street in Watertown? They're not on the list either, are they?
A. There were over 200 cell phones that were seized in this matter.
Q. You would agree, right, that the cell phones belonging to one of the two suspects are important pieces of evidence, right?
00:57 A. You mean during the course of the investigation or to date right now?
Q. In general. If the suspect -- one of the two suspects in the bombing has a cell phone, you understand that's going to be an important piece of evidence, a valuable piece of evidence, right?

A. It was during the course of the investigation at the very beginning, yes.
Q. Okay. Just trying to establish those are also not on this list, right, Tamerlan's phones?
A. I was not asked to verify any files from those devices.
Q. Understood. You would also agree with me that it can be important -- sometimes be important to know when a computer first began to operate or was manufactured, right?
A. I'm not sure I understand that question.
00:58 Q. Well, if you're trying to figure out when certain digital events on a computer happened and how that fits into an overall investigation, it can be a useful piece of information to know when the computer first came into existence as we know it, right?
A. When it was made by the manufacturer or when it was purchased from the store or when the owner bought it?
Q. Any number of those things. Any one of those facts could be a useful fact, right?
A. Potentially.
00:58 Q. The date Windows was installed on a Windows computer is an important fact to know in understanding where a particular device fits into the history of events, right?
A. Well, the Windows installation -- it depends. I would need to have more information in order to assess that. Windows installations -- you can actually install Windows multiple

times over the course of the life of a computer. So I could own a computer and do multiple installations of Windows. So I would have to have more information to --

Q. So you're not willing to say whether it's at least a piece of information that might be useful to know?

MR. CHAKRAVARTY: Your Honor, objection to the argumentative style both of this lack of concession as well as Mr. Fick's questions asserting facts not in evidence.

THE COURT: Overruled.

00:59 A. So could you repeat the question, please?

Q. Are you willing to acknowledge that the date Windows was installed on a computer could be an important piece of information to place the device in a time context relative to the investigation?

A. It is one piece of information that could be utilized.

Q. Okay. Let's actually make it a little bit more concrete. Now, I'm going to pull up Exhibit 1142-11. This is a document that describes or shows the date Windows was installed on the Sony VAIO, correct?

01:00 A. When that particular version of Windows, with that product key, yes.

Q. So that's the date here, 2/26/11, correct?

A. That's what's reported in the registry. That's from 11 --

Q. 1142-11, right?

A. Yes.

Q. Now, there's no evidence that any other version of Windows previously existed on the Sony VAIO, is there?
A. There's no evidence -- can you rephrase that or ask that question, please, again?
Q. There's no indication, no digital artifacts, on the Sony VAIO to indicate Windows was ever installed before this date, is there?
A. Yes, but there's also no to say that it wasn't.
Q. But as far as we know for purposes of this investigation, the Sony laptop, as we know it, Windows on that laptop was born on February 26, 2011, correct?
A. That particular version, that particular license, was on that date.
Q. Okay. And you're not aware of any evidence to suggest the computer existed earlier or that -- I'm sorry, that there was ever an earlier version of Windows, that the computer existed in some earlier form?
A. I haven't done the verification or analysis of that, no.
Q. You don't know the answer?
A. I haven't done the verification or analysis.
Q. As far as the evidence that's in the case then at least, the install date of Windows on the Sony was February 26, 2011, right?
A. This particular install of Windows, the date is collected as 2/26.

Q. And the Hewlett-Packard, the 2R14, from the family apartment in Cambridge -- I'm going to pull up 1143-08. This shows that the Windows install date on that computer was September 23, 2011, right?
A. Yes. Again, that particular license, that particular product key, that particular software, yes, that's what's collected in the registry.
Q. Again, there's no evidence, at least none you're aware of, to suggest that there was ever an earlier version of Windows on
01:02 that computer, correct?
A. That, I don't know. We'd have to do a further analysis for that.
Q. You don't know, in other words?
A. What I'm saying is we'd have to do further analysis to determine that.
Q. It's not something that was ever brought to your attention, right?
A. I was not asked to verify whether or not there were previously versions of Windows installed on the computer.
01:02 Q. Sitting here today, you are not aware of any evidence to suggest Windows ever previously existed on that computer?
A. I can tell you factually from the registry report here that this particular version of Windows was installed on that date.
Q. Okay. My question is: You're not aware of any evidence

to suggest that Windows was ever there earlier, correct?
A. Yes, but I'm also not aware whether it wasn't or not.
Q. I understand. But my question simply was: You're not aware of evidence that Windows was there earlier?
A. I have not done the analysis to determine whether there were previously versions of Windows on this computer.
Q. Now, as to the Samsung -- no -- yes, the Samsung, the Samsung from Laurel Street in Watertown, Tamerlan's computer, as you put it?
01:03 A. What number, sir?
Q. Going back to your exhibit -- I'm sorry, your chalk, so to speak, 1577, I believe, talking about the Samsung laptop, 1W3, Watertown.
A. So D385?
Q. D385. 1W3 is in parentheses, yes.
A. Yes. That type of analysis was not done -- I don't have access to that analysis for D385.
Q. Right. So my question is: Are you aware of when Windows was installed on that computer?
01:03 A. I'm not.
Q. Did you ever have an awareness of when Windows was installed on that computer?
A. I wasn't asked to verify or validate whether it was or was not.
MR. FICK: If I could just have the screen for the

witness, your Honor?
Q. Showing you a document and see if this helps you to answer the question. First of all, do you recognize, in general, what this kind of document is?
A. It's a security account manager information file.
Q. Does this help you answer the question, for example, of when the Windows administrator account on the 1W3 was installed?
A. The administrators account are typically a part of the
01:05 standard installation, so I'm not sure whether or not this was user created or whether or not it was machine generated.
Q. Does this enable you to say or does this enable you to agree with me that the Windows administrator account on the Samsung laptop was created on September 21, 2011?
MR. CHAKRAVARTY: Objection, your Honor. There's no foundation for what this document is, where it's from.
THE COURT: Sustained.
MR. FICK: If we can clear this, and we'll go back for everyone in the courtroom to see again Mr. Swindon's summary
01:06 exhibit. Are we back up?
Q. So just to review, we established, if I'm not mistaken, that the Sony VAIO Windows install was dated to February of 2011 just a few minutes ago, right?
A. If that's what was on that exhibit that you showed, then, yes.

Q. And we established that the HP Pavilion was September of 2011, right?
A. If that's from the exhibit report, then, yes.
Q. And you're unable to say, sitting here today, when the Samsung Windows install happened, right?
A. I don't have the information available to make that determination.
Q. Now, at the time the Sony VAIO Windows install happened in February of 2011, Mr. Tsarnaev was still a high school student, right?
A. I don't know that information.
Q. Well, I mean, you know things like the names of his friends, right?
A. I do. I am aware of some of his friends, yes.
Q. You know he was arrested after the Marathon bombings in 2013 when he was a sophomore at UMass Dartmouth, right?
A. I do.
Q. So back in 2011, two years prior, he would have still been in high school, correct?
A. I'm not sure the dates he was in high school.
Q. You're not aware of what, if any, computer the family might have shared on Norfolk Street before September of 2011 when the HP Windows was installed, right?
A. Can you reask that again, please?
Q. We established, I think, with you that the desktop

computer, the Hewlett-Packard, at Norfolk Street, Windows was installed on that computer in September of 2011, right?

A. We've established that Windows was installed on that computer, but that did not draw the conclusion that that's when the computer was brought into the house.

Q. You're not aware of any evidence that that computer existed earlier, right?

A. Not from the data that we have here, no.

Q. You're not aware of any other evidence to suggest if any computer existed earlier or if there was some other computer, right?

A. I don't have that information.

Q. You just don't know. But what we do know is that the Sony VAIO, the Windows install on that that we know about, was in February of 2011, right?

A. The Windows install from the registry shows that that install of Windows was done on that date on that computer.

Q. And that's two years prior to the time when Mr. Tsarnaev is a sophomore in college, right?

A. Again, I'm not aware of the dates when his -- what his student record was.

Q. Now, talking further about the Sony, you talked a little bit in your direct testimony about device attachments -- you remember that -- just a few minutes ago with Mr. Chakravarty?

A. I'm sorry. You said --

Q. Device attachments. You talked about finding the date -- that one date when the Kingston was inserted into the Sony?
A. That was one that we spoke on, yes.
Q. Were you aware that Tamerlan's HTC phone was connected to the Sony at least twice prior to September of 2011?
A. I wasn't asked to verify that piece of information.
Q. Is it something you ever came to learn in your investigation, in your work on the investigation?
A. There are multiple devices that were in the USB store
01:10 which comes out of the registry that were reported being plugged into 1R6.
Q. But you're not -- sitting here today, you're not aware whether Tamerlan's phone was attached twice prior to September?
A. I don't have that information in front of me to verify that.
Q. Do you know if anybody at the FBI ever dug that information out?
A. I'm aware that the registry was looked at and the USB-stored devices were looked at, yes.
01:10 Q. Was there some kind of written report prepared about that that you know of?
A. I don't have that to access. I don't recall.
Q. You don't know?
A. I don't recall.
Q. Are you aware that the Sony was used by multiple Skype

accounts, over the course of its existence, from your review of the Internet Evidence Finder reports?
A. I do know that the Skype was used by the defendant.
Q. Okay. Do you also know that Skype was used by an account called Bella Rizvan?
A. If you could pull up the report, I don't have the entire internet history memorized.
Q. So that's not something that you recall?
A. I don't have the report memorized.
01:11 Q. Do you have it with you?
A. Is it a part of the report that -- in the exhibit?
Q. Your report wasn't given to us. I'm asking you if you've got access to it.
MR. CHAKRAVARTY: Objection, your Honor. Your report wasn't given to us. This witness didn't draft a report. There's no evidence of any report.
THE COURT: Well, let's get -- we haven't even identified what the report is, so --
Q. Well, in your testimony last week, you talked about
01:11 reviewing the various computers with an application called Internet Evidence Finder, right?
A. Yes.
Q. And that extracts certain information about the computer's internet activity over its life, right?
A. It evaluates and parses out the internet activity from a

particular computer, yes.
Q. Among the things Internet Evidence Finder isolates are artifacts indicating or suggesting uses of Skype, correct?
A. It does have a social media component to it, yes.
Q. That includes Skype, right?
A. Yes.
Q. Skype is a communication program, voice and text-type messages between computers over the internet, right?
A. It's like a peer-to-peer video chat, yes.
01:12 Q. Okay. And you just said a minute ago you are aware that there was a log-in for Jahar Tsarnaev on Skype on the Sony, right?
A. Yes, because that was a part of one of the exhibits that we produced for 1R6.
Q. I'm asking you now: Are you also aware there was an account on there called Bella Rizvan on the Sony?
A. I was not asked to verify whether or not that account was on that computer.
Q. My question, sir, wasn't whether you were asked to verify
01:12 that. It's whether you know that from yourself looking, presumably recently, at the Internet Evidence Finder reports?
MR. CHAKRAVARTY: Objection, your Honor. Asked and --
THE COURT: Overruled.
A. I don't have that information here to make that determination.

Q. Whether or not you have it here in front of you now, do you recall seeing that information when you looked at the evidence --
A. I do not recall.
Q. You do not recall?
A. I do not recall.
Q. You do know that Bella is the name of one of Jahar's sisters, right?
A. I do not.
01:13 Q. So you know a friend of his from UMass Dartmouth is Giovanni Norgill, right? You said that last week?
A. I knew that from -- yes.
Q. You know that Dias Kadyrbayev is a friend of his, right?
A. I do know they were defendants in another matter, yes.
Q. You know that Katherine Tsarnaeva is Tamerlan's wife, right? You said that last week?
A. Yes.
Q. But you don't know that Jahar had a sister named Bella?
A. The part of the investigation that I was responsible for
01:13 had no dealings with other siblings.
Q. That name never came up in your work with people under your supervision about the electronic devices in the case?
MR. CHAKRAVARTY: Objection, your Honor.
THE COURT: You may answer it.
A. It did not.

Q. Now, I'm going to go to Exhibit 1142-01, which is the selected internet history from the VAIO. I'm going to zoom in on sort of part of it here, just the beginning.

Now, Exhibit 1142, this -- whoever created this called Key Internet History it's just one page, right? It's one page pulled out of the internet history?

A. It is one page pulled out of the -- generated from the Internet Evidence Finder.

Q. Okay. And so I think you said there was something like 30,000 internet history entries on the Sony, right?

A. I believe so, yes.

Q. And so this one-page selection is a very, very small part of that, right?

A. Yes, less than 30,000, yes.

Q. Substantially less?

A. Yes.

Q. And this was a selection made not by you but by the investigative team, right?

A. Yes.

Q. But in the process of verifying this, you went back for each -- if I understood your testimony, you went back for each of these line items and went to the internet history to confirm it's there, right?

A. Went to the internet history -- we went to the Internet Evidence Finder results.

Q. To confirm that everything in this spreadsheet is actually there?
A. We went to the results of the internet finder -- Internet Evidence Finder and -- yes, and confirmed that it was there.
Q. You've been saying "we" again. You said "we" a few times last week. When you say "we," do you really mean I, or were there multiple people doing it?
A. I was with John Petrozelli, the senior analyst.
Q. In verifying the spreadsheets line by line, you did that
01:15 together, is that fair to say?
A. Yes.
Q. But you personally participated in every aspect of it, correct?
A. Absolutely, yes.
Q. Now, in the process of verifying these items, you obviously saw the entirety of the internet history, correct?
A. These were subreports from the larger base, so we were confirming only what was on these reports.
Q. But in order to confirm them, you had to go back to the
01:16 original, to the collective, right?
A. The 30,000 entries?
Q. Yes.
A. Yes.
Q. And so, in the process of doing that, you had occasion to observe that the bulk of the internet history on the Sony was

activity on Facebook and VK, which is a Russian Facebook equivalent, right?

A. I'm sorry. What --

Q. Is it fair to say that the course of seeing the entire internet history --

A. Right.

Q. -- you could observe -- you did observe that the bulk of the internet history on the Sony was Facebook activity and VK.com activity, a Russian Facebook equivalent?

01:17 A. I'm not sure I can assess that sitting here. We went line by line to determine and validate and verify that this stuff was there. It was so voluminous, I couldn't tell you whether it was a percentage or not.

Q. You didn't even notice in passing where most of the web addresses were coming from on that giant collection?

A. We went to these entries to make sure that they were there and existed. As far as assessing what else was there, as far as a percentage in its totality, we did not.

Q. So you were narrowly focused on these entries, didn't even

01:17 notice anything else on the overall record you were reviewing?

A. Other than that there was other internet activity there, yes.

Q. Wasn't of interest to you where the predominant amount of internet activity was?

A. It was of interest to me to make sure this information

existed in those reports.
Q. That's your sole and narrow focus; is this information there? That's it?
A. That was my job, yes.
Q. In the course of your investigation earlier, in dealing with the people under your supervision who reviewed the Sony over the course of two years, did that topic ever come up?
A. Not specifically, no.
Q. Never had a discussion inside the FBI CART team about the
01:18 nature of the Sony's internet activity?
A. Not specifically the internet activity.
Q. Now, you're aware, correct, that the FBI did an analysis of the search history, the internet search history, on the Sony, right?
A. Some of those entries are included in these reports, yes.
Q. You are aware that the FBI did a separate analysis of the search history on the Sony, correct?
A. What type of search history?
Q. Well, let me just put more of a point on it. The 53-page
01:18 report we were talking about before in front of you that contains an analysis of the search history, correct?
A. Can you refer to what page that is, please?
Q. Sure, Page 46.
A. This looks like it's a collection of search terms.
Q. Right. So you testified that you're familiar with this

report, right?
A. In general, yes.
Q. You've seen it before, right?
A. Yes.
Q. Petrozelli and Nathans, the people who worked on it, are people you work with, right?
A. Yes.
Q. And so you're aware that the FBI did an analysis of search terms on the Sony that are indicative of his predominant
01:19 internet usage, right?
A. According to this report, yes.
Q. Well, you don't have any reason to think the report is wrong, do you?
A. No.
Q. And it's fair to say that the top two terms in the predominant search history are words that you might --
MR. CHAKRAVARTY: Objection.
Q. -- expect to see in the computer of an adolescent male?
THE COURT: Overrule.
01:19 A. Am I answering that question? Can you rephrase that again, please?
Q. The top two search terms are terms you would not be surprised to find in the computer of adolescent male, fair to say?
A. I'm not going to say that. I'm not an adolescent

psychologist, so I don't know whether or not an adolescent male would be searching for those terms.

Q. Among the top 16 search terms identified in this predominant usage chart is the single word "Chechnya," correct?

A. Yes.

Q. You're aware that the defendant's family, his paternal side of the family, comes from Chechnya, correct?

A. I'm aware they are from Chechnya, yes.

Q. Also fair to say that, among these top 16 predominant usage search terms, there is nothing about Islam or jihad?

01:20

MR. CHAKRAVARTY: Objection, your Honor.

THE COURT: Sustained.

Q. Now, I'm going to move on to Exhibit 1142-13.

A. Are we done with this report?

Q. For the moment. You can leave it on your desk if you'd like.

This is 1142-13, selected user files from the VAIO, correct?

A. Yes.

01:21

Q. And this is a report that's about four-and-a-half-pages long, correct?

A. Yes.

Q. And this is, again, a list of files selected by somebody on the investigative team, correct?

A. Yes.

Q. And in addition to the name and path of the file, if we go back to the top of the spreadsheet, there are these two columns here, "created in local time" and "file system record in local time." Do you see that?
A. Yes.
Q. It's correct, isn't it, that Windows maintains a variety of date-and-time information about files?
A. Yes.
Q. And that's -- there are certain descriptors or categories of each of the pieces of information Windows maintains, correct? One of them is "created"?
A. That's one of them, yes.
Q. "Modified"?
A. Yes.
Q. "Accessed"?
A. Yup.
Q. Something called "MFT entry modified," the "master file table entry modified"?
A. The "born on" date would be more appropriate.
Q. You're familiar with those categories of information that Windows holds about files, right?
A. Yes.
Q. And fair to say the meaning and significance of that data is not always intuitive or obvious?
A. It is to the forensic specialist but not to sort of the

general computer population.
Q. Okay. Now, the created date is, generally speaking, the date or time that the file appeared on the computer or device where the file is located, correct?
A. Depending on what versions of Windows, yes.
Q. And for the purposes of your chart here, which of the Windows time categories is file system record date in local time?
A. This was adjusted -- these were adjusted numbers for local
01:23 time. As we had talked about, some of them were --
Q. I want to break that down into two pieces. Put aside the time zone issue for a moment. What is meant by "file system record date"? That's not a term that shows up in Windows itself, right? So what do you mean?
A. That was an adjusted time for the time record, for the Zulu time.
Q. But both of these are local time, right? We have "created in local time," and we have "file system record date in local time," right? Both are local time?
01:24 A. If you could pull the thing out so I can see it in its entirety, please?
Q. Sure .
A. So the created local time -- sorry. What was your question again?
Q. I'm asking you about "file system record date in local

time." What is that? Which of the Windows time artifacts does that come from?
A. That is not a Windows time artifact. That was, like, with some of the -- several of the other spreadsheets, that was added by the analyst.
Q. So added by the analyst on what basis?
A. I didn't create the report. We determined that this is a user -- selected user file from the main directory listing report.
01:24 Q. Sir, you didn't create the report, but you verified the report, right?
A. I verified, yes, that the web cam media was created in local time, yes.
Q. How did you verify file system record date in local time if you can't tell me which Windows artifact it is?
A. When I sat with the analysts, we went over line by line to determine that the web cam media entry was in the directory listing, the main directory listing.
Q. So are you saying you did not verify the time entries in
01:25 the spreadsheets?
A. I did not create the file record time category.
Q. You didn't create the category. I'm asking if you verified it.
A. I verified with the person who created the report, yes.
Q. So what? They just told you it was correct?

A. I sat with the analyst, and we went through the main directory listing of what you're looking at here to determine that the created local time. And we sat with the -- the senior analyst that made this report, and we went over it line by line together, yes.

Q. I understand you verified created in local time with the analyst. What is file system record date in local time?

A. That's something that the analyst -- that is a -- something that the analyst made.

01:26 Q. Based on what?

A. I don't have that information in front of me.

Q. So when you sat with the analyst and verified the entries line by line, the question didn't come up: What is that?

A. There were over -- there were a number of different documents. I don't recall specifically this particular document.

Q. Well, apart from this particular document, these two categories, right, "created in local time" and "file system record date in local time," those are all over multiple

01:26 spreadsheets that you put into evidence with Mr. Chakravarty last week, right?

A. Yes.

Q. So what is "file system record date in local time"?

A. I would have to go back and ask the analyst. We went line by line to determine that the "created in local time" came from

the master file list and that the path of the files were there for selected user time.
Q. So bottom line is you can't answer that question sitting here today, What is file system record date?
A. I don't have the information in front of me to answer that question.
Q. You don't recall even knowing at the time you verified the spreadsheet?
A. We went over multiple spreadsheets over a period of three or four days.
Q. Right. But this category, file system record date on multiple spreadsheets, you don't remember what that is?
A. I don't recall.
Q. Okay. So then, certainly, you would agree then, since you don't know what it is, that the fact that the time the file was created and the time in the second column doesn't necessarily say anything about whether the file was ever opened?
A. The created in local time was when it was created on that --
Q. Right. So it's simply the fact that there's another column with a different time on it that's later doesn't mean the file was opened on that date because you don't even know what that column means, right?
A. I would have to get the information from the analyst to verify what that information is.

Q. It's at least fair to say that from this spreadsheet one cannot infer that the fact that there are two different times means this file was ever opened?
A. Exactly, or that it was not or that it was.
Q. Right. There's no information?
A. I don't have the information to determine that from this particular spreadsheet.
Q. Now, I want to go to a particular file on here. I'm going to expand it just by way of example. See this
01:28 fundamentalconcepts.pdf? See that?
A. Uh-huh.
Q. Created date, September 1, 2004?
A. Okay.
Q. That can't be right, can it?
A. Well, it could be. If it was created on another device, that creation date could have been carried over when it was populated from a removable media device.
Q. I thought you just told us a few minutes ago that all of the created dates here are the dates the file was created on
01:28 the Sony?
A. It's when the file was born with the exception of when something is done with removable media or downloaded from the internet.
Q. So your belief then is that this created in local time simply reflects when Fundamental Concepts might have been

created on some other device?
A. I don't have that information in front of me, but I would -- yes, based on the information here.
Q. Well, let's try comparing then to see what created certain looks like on the master file table for this item. If I can open Exhibit 1142-151, Page 1872, can you see that on your screen, fundamentalconcepts.pdf, and then the highlighted creation date?
A. Barely but -- can you zoom it out?
01:30 Q. You know, I think I might have to actually open it in PDF to do that. But one moment. Go to Page 1872; zoom. Here we have Fundamental Concepts. I thought I had it. Sorry. Fundamental Concepts, going across, across, across. Creation date of October 10, 2011.
A. Can you possibly bring up the other one, also, please, in the other report?
Q. Which one?
A. The original report we were --
Q. Yes, absolutely. So we will go back to that, which is
01:32 1142-13, Fundamental Concepts, September 1, 2004.
A. Can you go back to the other report again, please?
Q. Sure.
A. Okay.
Q. So the created file in the master list, the 4,000-plus page document, September 10, 2011, for Fundamental Concepts, on

your derivative -- or the FBI's derivative spreadsheet, it's the 2004 date?

A. There were multiple different types of applications used. This particular sheet that you're looking at was an X-Ways forensic file listing export, and that report could have been made from AD Labs.

Q. So there's -- a different software might give a different answer to a question to when a file was created on a computer?

A. Potentially, yes.

01:33 Q. What did you actually use when you verified the derivative exhibit, the one that showed 2004? How did you verify that date?

A. We used multiple data sets. One of them was we wanted to make sure that this entry -- that the file actually existed on the computer and that the entry was in the file listing.

Q. So you're saying you didn't verify the dates?

A. We didn't -- the information that we used at the time was -- could have been from the AD Labs. Could have been from the other product.

01:34 Q. So different products, you're saying, can give a different answer about when a file was created on a computer?

A. It's possible.

Q. Sitting here today, you don't know which is correct?

A. I don't know which is correct; I do not.

Q. It sort of stands to reason, though, that a computer where

Windows was installed in 2011 couldn't have had a file created on it in 2004, right?

A. Not unless that file was created someplace else, either the internet or a removable media and then copies to that device.

Q. But it still has a creation date, a date it was born on the device where it was --

A. Would be the born-on date, yes.

Q. As I understood it, the derivative spreadsheet was supposed to show, as I understood it, the date the file was born on the Sony, right?

A. I'm sorry. Can you ask that question again?

Q. As I understood the purpose of the derivative spreadsheet and your description of it a few minutes ago, that column is supposed to tell us when the file was born on that computer, right?

A. It was created in local time on that computer, yes. I'm sorry, when the file was created in local time.

Q. On that computer or not?

A. Not necessarily on that computer.

Q. Not necessarily, right?

A. Depending on how that file -- where that file was originally created from.

Q. So how do you know the difference? How can we interpret any one of these items what it means? Are you able to do that

sitting here today?
A. Not sitting here today, no. We would need further analysis on the file. The file does exist on the computer, and the file entry does exist on the directory listing.
Q. But you're not confident about the dates in these spreadsheets?
A. I don't think any forensic person would ever be a hundred percent confident in dates and times generated by the operating systems.
01:35 Q. I'm still curious. What happened when you tried to verify this date? You must not have compared it to the 4,000-page list that's in the exhibit because that has a different date, right?
A. Must be, yes.
Q. But sitting here today, you don't know what device output or what software output you used to make the verification?
A. Not for this particular spreadsheet, no.
Q. For any of the spreadsheets, can you say where the data came from?
01:36 A. We had -- there were hundreds of files, and there were at least 50 or 60 spreadsheets that we were verifying.
Q. So you didn't have a standard procedure to verify the dates and times in the spreadsheets?
A. There was no standard procedure because it was a bunch of different types of devices. It was cell phones, thumb drives,

hard drives.
Q. Let's just stick with computers. Did you have a standard operating procedure to verify dates and times for lists of files from computers?
A. There was no standard procedure, no.
Q. Just to -- this is not an isolated problem, fair to say?
A. I can't determine that with the information in front of me.
Q. Well, let's take a look at a couple more examples at
01:37 least. I'm going to go to Page -- well, there's the next one right here, fundamentalconcepts.pdf, February 14, 2006. That's also a date that's like -- something like five years before the Windows install on the Sony, right?
A. If the -- the 2011 date, when that particular install of Windows, yes.
Q. So certainly would raise a question in your mind: How is it that a file could be created on the Sony in 2006, right?
A. That file could have been created on the internet in 2006 and then put on the Sony --
01:37 Q. Again, it's just --
A. -- in 2011.
Q. It's just an example of that date doesn't necessarily reflect the creation date on the Sony?
A. Depending on what type of file it is, where that file was created, it may not reflect when it was created on the Sony.

Q. Just as a point of comparison, going to the master file table for that file, the Exhibit 1142-151, Page 150.
A. That's not the master file table, but it is a directory listing.
Q. For purposes of the exhibit in this case, there was a 4,000-plus-page exhibit which you represented to be a complete list of all the files on the Sony, right?
A. That's the complete list that the software product produces, yes.
01:38 Q. And so if we go to that list and look for the fivegrounrules.pdf document, we again see a September 2011 creation date rather than a 2006 date, right?
A. Can you blow that up a little, please?
Q. Go to Page 150. Here we go. Five Ground Rules. Scroll across. We get a date September 10, 2011, again, right?
A. Yes.
Q. So the created data in this file listing doesn't match the created data on the FBI's derivative exhibit again, right?
A. That data is different, yes.
01:39 Q. So fair to say it would not be appropriate to rely on the derivative exhibit, which is 1142-13, to figure out what date a file might have appeared on the Sony VAIO?
A. We'd rely on -- yes. I would rely on the master file -- I mean, the complete list.
Q. Okay. Now, if I'm hearing you, you're saying the complete

list is correct?
A. The complete list is generated by the approved software tool.
Q. So the derivative list was generated by some unapproved software tool?
A. No. The generated list was created by the senior analyst and the examiner that worked with him.
Q. Out of the air or they used some tool?
A. They used multiple different pieces of information.
01:40 That's why it's called derivative.
Q. Okay. They used an unapproved tool to create the derivative exhibit?
A. I'm not sure specifically what tool -- I mean, they used -- it's an Excel spreadsheet, but the data came from multiple different data sets as processed by the evidence -- or the evidence was processed by.
Q. You don't know what tool was used to generate the data on the derivative spreadsheet, one, right?
A. I'm not sure a tool was used to generate the derivative
01:40 spreadsheet. The information came from multiple places to get to the derivative spreadsheet.
Q. Wherever it came from, you don't know where it came from?
A. I don't have it in front of me to make that determination.
Q. Okay. And the authoritative, I guess, you're saying, table, you didn't -- in the process of verifying the derivative

spreadsheet, you didn't check that data against the authoritative table?
A. That file creation date could have been from AD Labs. Again, we used multiple tools for this to create these derivative spreadsheets.
Q. So the tools conflict with each other?
A. Possibly, yeah.
Q. So --
A. Depending on --
01:41 Q. Where does that leave the bottom line? What's your -- as an expert computer forensic examiner on the witness stand today, which set of data can we rely on? The complete list we've got up on the screen here showing September 11th or the derivative list showing a date in 2006? Can we rely on either of them?
A. It depends on what you're trying to determine.
Q. If you're trying to determine when a file will appear or was created on the Sony VAIO, what would you rely on?
A. I would rely on the master file list.
01:42 Q. Which is the thing that's on the screen right now?
A. The thing that's on the screen right now, yes.
Q. So if that's what the reliable source is, why didn't you verify the derivative evidence against the reliable source?
A. That derivative evidence could have been when that file was created in another location.

Q. But if that's not what the exhibit is supposed to be portraying, why wouldn't you correct it?
A. I'm not sure that that's accurate. If you pull it up, it doesn't say created on the 1R6. It just says "file created."
Q. The spreadsheet doesn't say anything about what created means. That's why I asked you initially. If I understood you correctly, your initial response was created means the date it was born on the Sony.
A. No, I did not say that.
01:42 Q. Okay. At least we're clear now. Created date on those derivative listings is not a reliable way to assess when a file appeared on the Sony?
A. Creation date was when that file was created, not -- it would not be indicative of when it potentially could have been created on the Sony, yes.
Q. It would not be indicative of when it potentially could have been created on the Sony, okay.
Now, I'm going to return to discussing a few more big-picture things about some of these devices. I'm going to
01:43 go back to your list, 1577 -- I'm sorry, 1557. I'm going to talk about the Samsung a little bit here again, the 1W3, D385. Do you see that?
A. Yes.
Q. Now, you testified last week that the FBI concluded that this was, in fact, Tamerlan's laptop computer, correct?

A. I testified that we were aware that it was Tamerlan's computer, yes.
Q. And you know that both from your understanding of what was found on the computer itself and other investigative information, correct?
A. Yeah. I did a cursory -- as a part of this process, did a cursory look of D385.
Q. You're also aware of other investigative information that ties the computer to Tamerlan, right?
01:44 A. I'm not -- I don't know what specifically you're referring to but in the general course of the investigation, yes.
Q. Well, you are aware, for example, it was found in a computer bag with his high school diploma, right?
A. I'm aware that it was found in a computer bag. I don't know what the rest of the contents of the bag were, but I am aware that it was a computer bag.
Q. You're aware that the computer was connected to the internet in Russia multiple times between January and July of 2012 when Tamerlan was there, right?
01:44 A. I don't have that information in front of me to determine that.
Q. Well, is that something you ever became aware of in your work on this investigation?
A. Not me personally, no.
Q. You never became aware of information that Tamerlan

traveled to Russia from January to July of 2012?

MR. CHAKRAVARTY: Objection, your Honor.

THE COURT: Overruled. You may have it.

A. I'm not sure that that's what you asked me. I think you asked me if whether or not the computer was connected to the internet when he was traveling in Russia.

Q. Let's take it step by step. Are you aware of information that Tamerlan Tsarnaev traveled to Russia between January 21 and July 17 of 2012?

01:45 A. I'm aware that Tamerlan traveled to Russia, yes.

Q. In roughly that time frame?

A. In roughly that time frame, yes.

Q. And are you aware that there are digital artifacts on the Samsung showing that that computer was connected to the internet in Russia during that time frame?

A. I do not have that information in front of me, nor am I aware of that.

Q. You never were aware of that?

A. I was never aware of that.

01:45 Q. Are you aware that the web history on the Samsung includes information about Tamerlan's log-in to multiple accounts associated with him?

MR. CHAKRAVARTY: Objection, your Honor.

THE COURT: Sustained.

Q. You said you did a cursory review of the Samsung in

connection with preparing for your testimony here, correct?
A. I did a cursory review of the computer because it was listed on this evidence sheet, yes.
Q. And during the course of the last two years, you supervised individuals who worked on the analysis of this computer, correct?
A. That's correct.
Q. And you over that time became aware of things that they were doing and finding, correct?
01:46 A. I'm aware of what they were doing in general, yes, as a supervisor.
Q. Particular findings were never brought to your attention?
A. Specific findings, no.
Q. Reports that they wrote -- that the people under your supervision wrote about the Samsung were never brought to your attention?
A. Other than through the general approval process, I don't have the specifics of the reports in front of me.
Q. Well, again, part of the general approval process, you're
01:47 the supervisor. You would review reports written by the people you supervise, correct?
A. Yes.
Q. That would include reports that people you supervise wrote about the Samsung, correct?
A. Reports that -- any reports that they would write, yes.

Q. Okay. And that's a normal kind of thing that you would rely on in the course of your work as a supervisor, correct?
A. Rely on for what, sir?
Q. Rely on for performing your duties.
A. Rely on -- I think the relationship as a supervisor of the forensic team is a little different than normal. The forensic person is actually assigned to the investigation, so any investigation subject matter would be decided or run by the case agents. I would make sure -- mine is more day-to-day
01:47 operations. Mine is: Did you come in to work on time? Is your -- you know, type of information.
Q. You still have occasion to read the reports that the analysts write about the Samsung, correct?
A. The forensic examiners write, yes, not the analysts.
Q. The forensic analysts write reports about their findings to pass them along to others in the FBI and the prosecution team to know what the evidence means, correct?
A. Their technical reports, if they worked for me, would go through me, yes.
01:48 Q. They go through you, and they go from you to investigating agents, case agents, prosecutors, and the like, correct? That's the reason they exist?
A. They would go to the case file. I'm not sure where they would be distributed from there.
Q. So you don't know whether the reports that your

subordinates write about important pieces of digital evidence ever see the light of day?
A. I approve them for accuracy and make -- and then once they're uploaded to the file, within the case file, I'm -- I don't make the investigative decisions on any particular case.
Q. Well, you did tell Mr. Chakravarty, right, that you're aware from your exposure to the Samsung over the last two years that a lot of similar kinds of files to those on the Sony were on the Samsung, correct?
01:49 A. Actually, I think I said, in the course of reviewing the evidence and validating, verifying for the trial, I am aware of a cursory look of D385.
Q. Okay. So you became aware, if you weren't already aware, that a lot of the same kinds of material is also on the Samsung, right?
A. Yes.
Q. And you also talked about the fact that there is encryption software on the Samsung, correct?
A. I talked about I was aware that there was a TrueCrypt
01:49 volume on the drive, yes.
Q. And TrueCrypt is a very powerful piece of encryption software, fair to say?
A. I'm not sure I would characterize it as powerful, but it's a freeware product that anybody can download to encrypt data.
Q. Well, if one has a good password in TrueCrypt, it's pretty

hard, even for very sophisticated tools, to get inside, right?
A. If the software is configured properly and the password is strong enough, it would be difficult, yes.
Q. Even for the most sophisticated U.S. Government tools, very difficult, right?
A. For the purposes of this, yes.
Q. But you understand, because you supervised the people who did it, that it was possible to get into Tamerlan's encrypted volumes because he had a bad password, right?
01:50 A. No, I'm not aware of that.
Q. You're not away the password was Allahu Akbar, with a number after it?
A. I'm not.
Q. You don't know how FBI analysts managed to find out what was in the encrypted volumes on Tamerlan's computer?
A. I'm aware that they are able to access that. I'm not aware how they were able to get the password.
Q. Now, fair to say that the use of encryption is considered something -- in investigative terms, it's considered tradecraft
01:50 when it's used by terrorists or criminals, right?
A. I'm not sure I can make that assessment.
Q. As a trained FBI agent, that's not the kind of assessment you would make?
A. What's that?
Q. Well, what constitutes tradecraft for criminals or

terrorists.
A. I mean, that's a very easy question with a very long answer. Tradecraft can be a number of different things.
Q. Is it fair to say that the use of encryption by a terrorism suspect is an example of tradecraft?
A. I'm not aware of any terrorism suspects that have used encryption, so I'm not sure I can answer that question.
Q. Well, are you aware that *Inspire Magazine*, one of the ones that you talked about with Mr. Chakravarty last week, recommends that people who want to engage in terrorism should use encryption?
A. I'm not aware of that, no.
Q. I'm just going to pull up a copy of Exhibit 1475-22.
MR. CHAKRAVARTY: Objection, your Honor. This is not impeachment.
THE COURT: Sustained.
If this is a pausing to go to a new thing, it's 11:00. We'll take the morning recess.
MR. FICK: Sure. Thank you.
(Recess taken at 11:02 a.m.)
THE CLERK: All rise for the Court and the jury.
(The Court and jury enter the courtroom at 11:28 a.m.)
THE CLERK: Be seated.
THE COURT: Mr. Fick?
MR. FICK: Yes, your Honor. Thank you.

BY MR. FICK:

Q. So good morning again, Agent Swindon.

A. Good morning.

Q. Just a few more questions about your knowledge of the Samsung laptop here among the devices seized, Tamerlan's laptop. We talked a bit about TrueCrypt a few minutes ago. Do you remember that? That's the encryption software?

A. Yes.

Q. It's true, isn't it that TrueCrypt is not among the

02:19 software on the Sony VAIO?

A. I'm not aware of TrueCrypt being on the Sony VAIO, no.

Q. Well, and, in fact, you introduced last week an exhibit listing all of the software on the Sony VAIO, correct?

A. Yes.

Q. And that list did not include TrueCrypt, correct?

A. It did not include TrueCrypt, yes.

Q. So it's not just that you're not aware of TrueCrypt being on the Sony VAIO, in fact, TrueCrypt is not on the Sony VAIO?

A. TrueCrypt is not on the Sony VAIO.

02:19 Q. Thank you.

Now, in the course of your cursory review of the Samsung, or previously in your work as the supervisor of the CART team, did you ever have occasion to see what the desktop of the Samsung looked like, the wallpaper, the background, all of that?

A. On D385.
Q. On the Samsung, Tamerlan's laptop?
A. No.
Q. You never saw what the desktop looked like?
A. I never saw what the desktop looked like.
Q. Did your cursory review of the Samsung include the Internet history of the Samsung?
MR. CHAKRAVARTY: Objection, your Honor, to going through each of the portions of --
02:20 THE COURT: Yes, sustained.
MR. FICK: I'm sorry?
THE COURT: Sustained.
MR. FICK: I'm not sure what the objection was.
THE COURT: I take it as relevance.
MR. FICK: May we approach?
THE COURT: All right.
(Discussion at sidebar and out of the hearing of the jury:)
MR. FICK: So two things: I would suggest, first of
02:20 all, the government opened the door to at least probe the witness's knowledge of the Samsung by itself, the prosecution, asking questions about what he knew about the Samsung.
Second, this is going nowhere near mitigation evidence. This is strictly evidence about the crime itself and the potential motives of the crime.

THE COURT: How?

MR. FICK: Information about the contents of Tamerlan's laptop and how that reflects on his state of mind. Potential preparation of the crime is evidence of the crime, of the motive.

MR. CHAKRAVARTY: I understand Mr. Fick saying it goes to Tamerlan's state of mind, evidence that might be on his computer that this witness, the computer forensic specialist who didn't even verify that information would somehow be capturing Tamerlan -- the coconspirator's state of mind when there's no evidence that this defendant had any access, knew what was on there or even that some of these questions about where the surface tree was and some of those things. I don't think the defendant's argument is that the defendant participated in that; in fact, it's just the opposite. They're suggesting that Tamerlan was doing a bunch of other things that the defendant was not. All that is outside this witness's basis of knowledge with regards to the device as well as it's not relevant to the conspiracy charge.

MR. FICK: I'm asking the witness questions about what he knows about what's on the computer.

THE COURT: And so what issue does that go to?

MR. FICK: It goes to Tamerlan's role in the conspiracy, among other things. I mean, it's evidence of --

THE COURT: Well, that sounds inculpatory; in other

words, it goes to prove the offense is a conspiracy.

MR. FICK: Well, there's no requirement, I would suggest, that the defense is only ever allowed to elicit exculpatory evidence. I mean, if it's evidence of the crime, if it's evidence of a motive of a coconspirator, it is relevant to the case, and simply the fact that we happen to be the defense of one of the conspirators does not mean that we can't elicit evidence about the offense to put in the context and to correct the misimpression that the government's presentation is making.

02:22

MR. CHAKRAVARTY: Right there it's motive evidence. The motive evidence is to the extent that the government is offering to show that was not the defendant's motive is one thing, but to show alternative motives or in this case that the motive was even greater for the coconspirator seems to be a relative culpability issue and has nothing to do with --

MR. FICK: Relative culpability matters in terms of correcting misimpressions that the government's presentation of the case is creating at this stage of the case. It's evidence about the offense, it's evidence about the alleged offender that is specifically tied to not only the motive for the crime but what he did in terms of committing the crimes.

02:23

THE COURT: No. Excluded.

(In open court:)

BY MR. FICK:

Q. So, Agent Swindon, I'd like to talk a little bit now about how one traces the history of when a USB device was attached to a computer, okay?
A. Okay.
Q. Okay? So you've heard of something called SetupAPI is a registry artifact in Windows. You're aware of that?
A. I have to look at the registry report, but I believe it is one of the categories in a registry report, yes.
Q. Right. And that captures information about when a USB memory device is plugged into a computer for the first time, correct?
A. I'm not sure what the chronological of events are, but I do know there is information stored there, yes.
Q. SetupAPI stores information about USB device attachments into a computer?
A. I would have to test that. I don't have that information in front of me.
Q. Well, I'm not talking about a specific computer, I'm talking about the methodology of doing the investigation now, okay? So as a general matter, SetupAPI contains date and time information about when a device is first plugged into a computer, correct?
A. You have to pull that up so I can see a registry report to see what you're referring to.
Q. So you don't know what SetupAPI is sitting here today?

A. I'm familiar with it. It's an entry in the USB report that comes from the registry, yes.
Q. And so you're not aware that that records the first time a USB device is attached?
A. It records when it is attached. I'd have to see the report to know that that is the first time that was in that.
Q. The registry, apart from SetupAPI, also contains other information about incident -- incidents when a USB is attached, correct?
02:25 A. Yes, it does.
Q. Okay. Now, these two sources I've mentioned, the SetupAPI and other data in the registry, actually record the event of the attachment, right?
A. It would be the physical attachment or the physical putting of the USB drive into that particular machine.
Q. And in addition to those pieces of data, there's -- there are also artifacts called shortcuts and links that I think you testified about with Mr. Chakravarty, right?
A. Yes.
02:25 Q. Okay. And shortcuts and links and jump lists contain information about files that a user may have accessed on a USB device, right?
A. Among other things, but yes.
Q. Okay. So those record information about the files themselves, not the event of the USB connecting, correct?

A. It could be the same event. But, yes, it does capture the file information.
Q. So in other words, you might be able to infer something about when a USB was attached from the jump list or link information but that's -- the jump list or link information itself records information about the file on the USB storage device, right?
A. Right. So just for clarification, the registry contains the information about the hardware and the connection of when
02:26 that piece of hardware went into that particular computer as opposed to the link file is going to have information regarding a file or files or folder that was accessed on that removable drive.
Q. Right. So those are -- they're related but different things, right?
A. Yes.
Q. Okay. So I'm going to pull up Exhibit 1142-02 which is the exhibit called "External Device Access on the Sony." You remember this spreadsheet that you talked about with
02:27 Mr. Chakravarty, right?
A. I do, yes.
Q. Okay. And this spreadsheet is based on jump list and shortcut data about files that were viewed on the Sony that were located on external devices, correct?
A. These are the information from the jump list records that

existed on the computer, yes.
Q. Okay. Jump list and shortcut records?
A. Yes.
Q. Okay. So this is not a listing of the device attachment registry information?
A. It includes some of the same information but it is not the registry report.
Q. It's not the registry report about the event of the device attachment, it's information about the files that were viewed on the external devices?
A. Yes.
Q. Okay. Now, the creation date for each of these entries is the date the file was created on the external device, correct, because these are jump lists and links, right?
A. I believe this might be the creation date of the actual link file. Let's see. 1B shortcut.
Q. Do you know?
A. Can you give me a minute because this is the only -- this is a -- a derivative report does not include all the information. So I would need to see the file, the information about the file, and then also the information about the Kingston thumb drive and the registry to determine that.
Q. Well, this is a spreadsheet that you reviewed and deemed to be accurate enough to include in an exhibit, correct?
A. Yes.

Q. So sitting here today, you don't know what the creation date column refers to?
A. I would need the other two pieces of information that we verified this with to determine that.
Q. Sitting here today you don't remember what those other two pieces of information were?
A. We verified hundreds of pieces of information on various spreadsheets.
Q. Okay. So sitting here you cannot tell me, then, whether this is the creation date of the file on the thumb drive or whether it's the date the thumb drive was inserted in the computer?
A. Not without the supporting information.
Q. You just don't know?
A. Not without the supporting information.
Q. Okay. Now, this Patriot thumb drive here, I believe you talked about that with Mr. Chakravarty, the serial number reflected there, that's not the same as the Patriot thumb drive that was recovered in the investigation and was included as an exhibit, correct?
A. This is the -- you're talking about the volume serial number?
Q. Right.
A. Yes, that is not the Patriot that was --
Q. And, in fact, this Patriot thumb drive with this volume

serial number was never recovered in the investigation, was it?
A. I don't have it, no.
Q. You're not aware of it being recovered?
A. I'm not aware of it being recovered.
Q. Now, do you know whether the FBI ever traced the artifacts from this missing Patriot across all of the electronic devices in the case?
A. I'm not sure I understand the question.
Q. Well, for example, what we have here on this chart
02:30 reflected in the first line is a data artifact taken from the Sony about this particular Patriot thumb drive at a particular point in time, right?
A. Yes.
Q. At some point in time, it was attached to the Sony and this file on the Patriot thumb drive was viewed from the Sony, right?
A. Yes.
Q. Okay. Now, did the FBI, to your knowledge, do any investigation of whether this Patriot thumb drive, the missing
02:30 Patriot, was attached to other devices seized in the case?
A. I believe that there was an analysis done on that, yes.
Q. And was any kind of writing produced from that analysis?
A. I don't have access to that report.
Q. Do you know whether --
A. Or a report.

I don't know.
Q. Now, another one of the devices you talked about was the Hewlett Packard desktop computer seized from 410 Norfolk Street, the Tsarnaev family apartment. You remember that?
A. If you could bring it up to reference it, yes.
Q. Of course. I'm bringing back up 1557. The second line here, 2R14, HP Pavilion, 410 Norfolk, that's a desktop computer seized from 410 Norfolk Street, the Tsarnaev family apartment in Cambridge, correct?
02:31 A. It was seized from 410 Norfolk, yes.
Q. Okay. And I think you testified on direct with Mr. Chakravarty last week that you acknowledge -- the FBI acknowledges that that computer was used by many people, right?
A. I believe people -- yeah, many people had access to that computer, yes.
Q. A large number of Tsarnaev family members at various times lived in that apartment, right?
A. I don't know. "Large" isn't a number. I'm not sure that we were able to determine how many, whether small or large, who
02:32 had access to that computer.
Q. Well, you testified that you're aware of Tamerlan's wife Katherine, who she is, right?
A. Yes.
Q. You heard the name, Jahar's father, Anzor?
A. Only from the computer username.

Q. You have no other knowledge of his father's name being Anzor from the investigation?
A. I don't. I don't.
Q. Ever heard of his mother, Zubeidat?
A. I didn't have anything to do with his parents in this investigation.
Q. So you know a number of people had access to the computer at 410 Norfolk Street, this computer, but you don't know who that might have been?
02:32 A. Not from the information in front of me, I can't determine that, no.
Q. Well, apart from the information in front of you, from your knowledge of the investigation, being a supervisor of the CART team for two years -- for the last two years, do you know anything about that?
A. Well, there are a number of pieces of information we would use to determine access to a computer. We would use the username that's associated with the computer. There would also be pattern-of-life investigative information that we would use.
02:33 And then there would be email access, Skype access and different types of maybe social media or access that we would be able to determine who was using that computer.
Q. And when you say "pattern-of-life information," that's information developed from the investigation about people who may have had access to the computer, right?

A. It's more -- not specifically the computer but pattern of life would be when somebody comes and goes either for work or for school or --

Q. And your testimony was you do know that multiple people had access to this computer, right?

A. Yes.

Q. But you don't know who -- you can't sort of list for me who that might have been?

A. I can't specifically tell you who specifically had access to that computer.

Q. Now, one of the artifacts that you looked at in Exhibit 1143-01, which I will pull up here -- these are exhibits in evidence. I'm going to go to 1143, 1143-01. You testified about an artifact in this derivative spreadsheet noting that on January 1st at 2013 at 1:47 a.m. there was a log in to Yahoo email for Jahar Tsarnaev. Do you see that?

A. I do see that, yes.

Q. Isn't it true that that is the one and only time there is any record on this computer of that email account being accessed?

A. I don't have that information in front of me.

Q. And apart from it being in front of you, do you know that to be true or not?

A. I don't know that to be true.

Q. But you don't know that is not true?

A. I don't know it's not true.
Q. Sitting here today you can't say whether there was ever another occasion on which Jahar Tsarnaev's email was accessed from that computer?
A. I don't have the information in front of me to make that determination.
Q. Did anyone ever ask you to make that determination?
A. No.
Q. And I'm going to also open 1143-05A, which is a derivative
02:36 spreadsheet -- sorry. One moment. Bear with me one moment.
(Pause.)
Q. So 1143-05A is the complete -- well, it's the lengthy 2,000 page or so long complete spreadsheet of the files from the Hewlett-Packard computer at 410 Norfolk, correct?
A. It was generated, yes, by X-Ways Forensics, yes.
Q. And I just want to draw your attention to the date and time information that's generated on this spreadsheet on this computer. You see there's some -- some of the date and time information has real, like, normal dates and times after it.
02:37 Do you see that? And then some of the same columns have information that does not appear to be in the format of a date or time?
A. Okay. That's what -- that's what this -- you're displaying, yes.
Q. Well, that's what was submitted to the Court as an

exhibit, right?
A. The complete list was -- the complete list that X-Ways Forensics generated was provided as an exhibit, yes.
Q. And that's what this is, right?
A. If you're looking at --
Q. 1145- -- 1143-005A?
A. Okay.
Q. So at least in this form, this spreadsheet could not be used to verify any of the filed time data in your derivative
02:38 spreadsheet because it's missing --
A. I'm not sure all of the columns have the time and date listed the way that it is but, again, we used both AD Labs and X-Ways Forensics to verify the information.
Q. Do you know which one you used in this particular instance?
A. I do not know which one.
Q. Can you explain why this particular tool generated date and time information that's not comprehensible?
A. I don't know.
02:38 Q. I'm going to go now to Exhibit 1150 which is the Kingston thumb drive found in the landfill that you talked about. Do you remember that? Do you remember talking about that?
A. If you could bring up the spreadsheet again we could confirm.
Q. Hold on. Exhibit 1145-01 -- I'm sorry -- 1150-01.

Now, the bulk of the files that you talked about on this thumb drive were carved; in other words, they were recovered from deleted space, correct?
A. They were either recovered or carved, yes.
Q. And when we see this path, "path unknown" with all of that -- those numbers, et cetera, directory markers before the file name, that's an indication that the file was carved, right?
A. Using this particular software product, yes, it would tell
02:39 you that -- that CL is a cluster number of where that file was located or started.
Q. And there's no way to know when the files were deleted off that thumb drive, correct?
A. There's not. As again, with carved and deleted files, it's more of access for investigative purposes than it is for the date and timestamps.
Q. And one of the carved items retrieved from this thumb drive, Exhibit 1150-09, was a rental application from Katherine Tsarnaev, correct?
02:40 A. Yes.
Q. Okay. And a few pages in it includes her pay stub, right?
A. If that's '09, then yes.
Q. Let's talk a little bit more about 1475 which is the hard drive seized from the street in Watertown. The derivative file listing for that exhibit -- actually, rather than showing you

the file listing, what I think I'm going to do is go to the file directory here.

Now, you testified last week and I think today that these four folders at the top here actually existed in that form on that hard drive, right?

A. Yes, I believe so. Yes.

Q. And this English paper that's still listed on the top here, that actually was not visible in the hard drive as an active file at the time it was seized. That, in fact, was carved from having been deleted at some point in the past, correct?

A. Yes.

Q. And the hard drive sort of contains a kind of greatest hits collection, right? There's Awlaki materials, audio files in that first folder, right?

A. I'm not sure what you mean by "greatest hits" but --

Q. Well, a lot of files that we've seen on -- that you talked about from the Sony and other devices, a lot of those files -- a very large number of them are all here collected together on this hard drive from Laurel Street in Watertown. Is that right?

A. Can you slide the screen over so I can see the next half?

Q. I'm sorry. So that's a collection of Awlaki audio files, correct?

A. Those are a collection of Awlaki files, yes.

Q. And there are these Russian textbooks about explosives, et cetera, right?
A. There are Russian textbooks in there, yes.
Q. Well, and you remember looking at the translations from the derivative file exhibit that the titles have to do with explosives and munitions and that kind of thing, right?
A. You're going to refer to each of them specifically or do you want --
Q. Well, as a general category. You've looked at the
02:43 translations of these titles in your spreadsheet, right?
A. Well, yeah. Do you want to make reference back to that or are you asking --
Q. I'm trying to ask some general questions about the category, the type of materials first. If you want to look at the list, we can.
A. Well, if you'd like to ask me specifically, I can comment on --
Q. Well, the first thing I want to do is ask as a general matter this collection of DjVu e-reader files in Russian, it's
02:44 a collection of lengthy texts about explosives and munitions, correct?
A. We can go through each one and look at the top page and I can tell you --
Q. Well, your own exhibit, the derivative exhibit, contains translations in the side, right, titles include "Detonation of

Explosive Media," "Physics of Explosion and Impact," "Blast Effects of Explosions," "Initiating Explosive Substances," et cetera, right? Those are the titles of those files, correct?

A. Yes.

Q. And you testified that carved artifacts of those files were found on one of the thumb drives, right?

A. Yes.

Q. But it's true, isn't it, that none of these files or any artifacts reflecting these files exist on the Sony VAIO computer?

A. I'd have to go back to the information that we have, but I don't have that all committed to memory. I mean, I do know they existed here. If you would like to go back and look at the file listing we can identify whether or not they were there.

Q. As far as you know sitting here today it's true, isn't it, or at least as far as you can recall, that these files do not exist on the Sony VAIO?

A. I don't know that for a fact. I would have to go back and look at the listing.

Q. You don't know?

A. I don't have the information to make that determination.

Q. Okay. Now, in addition to those materials, there's a collection of *Inspire* magazines as well, right?

A. Yes.

Q. Okay. And there were also some files on the top level of this hard drive that -- when it was recovered that were not included in this exhibit, correct?
A. I think there were. I was asked to verify these to make sure that they existed.
Q. Okay. I just want to pull out some things from the complete file listing just to nail that down.
Pulling up a page out of 1475-02A, which is the complete file listing from this drive, there were some other items at the top level of the drive that are highlighted in yellow here that we have seen on other exhibits but that also were on this hard drive recovered in Watertown, correct?
A. Yes. If this is from 02A, then, yes, that is a directory listing from the drive.
Q. So "Book of the End," "Join the Caravan," those are all on, as well, the top level of this hard drive when it was recovered, correct?
A. Apparently so, yes.
Q. And further down the file list you're aware that there are a couple of Russian language documents also on the top level of this drive when it was recovered, correct?
A. Yes.
Q. And these are documents that have Russian language instructions about making explosives, correct?
A. I don't know that.

Q. You don't know what these files have?
A. No, I did not look in the translation for those files.
Q. Did anybody under your supervision at the CART team of the FBI ever find out what was in those files?
A. Not that I'm aware of.
MR. CHAKRAVARTY: Objection, your Honor.
THE COURT: No, it may stand.
BY MR. FICK:
Q. Now, isn't it true that this hard drive retrieved on Laurel Street in Watertown was formatted by Tamerlan's Samsung computer?
A. I don't have the information to determine that.
Q. You don't know?
A. I do not have the information to determine that.
Q. Well, whether you have it in front of you now, do you know from anything you ever did in the case whether that is true?
A. I don't have the information in front of me to confirm that.
Q. Again, putting apart what you do or don't have in front of you, did you ever become aware from your work on this case as a supervisor of the Boston CART team whether Tamerlan's computer was the computer that formatted this hard drive?
A. I don't have that information to be able to make that determination.
Q. Again, I'm asking not only about today but whether you

ever came to know -- or whether this was true in the past?
A. No.
Q. You don't know?
A. I don't know.
Q. Do you know whether anybody else at the FBI checked?
A. Checked what, sir?
Q. Checked to see what computer formatted this hard drive.
A. No.
Q. Isn't it true that every single file and folder on this
02:48 hard drive is owned by Tamerlan's computer, using the "owner"
as used in Windows parlance?
MR. CHAKRAVARTY: Objection, your Honor.
THE COURT: Overruled.
You may answer it.
THE WITNESS: Again, I don't have that information to be able to make that determination nor did I, you know, validate or verify that.
BY MR. FICK:
Q. Well, whether you have it in front of you now or validated
02:48 it or verified it, did you ever become aware in your role as a supervisor of the CART team in Boston that every single file and folder on this hard drive was created by Tamerlan's Samsung computer?
A. No.
Q. You never became aware of that?

A. No.
Q. Do you know whether anyone else at the FBI ever became aware of that?
A. I'm not aware of that.
MR. FICK: If I may have one moment, your Honor?
(Counsel confer off the record.)
MR. FICK: I have nothing further.
MR. CHAKRAVARTY: Just briefly, your Honor.

REDIRECT EXAMINATION

02:49 BY MR. CHAKRAVARTY:
Q. Agent Swindon, you were asked several questions about different pieces of information on different devices, that you weren't able to recall whether that information that Mr. Fick asked you was, in fact, on those devices. Can you explain for the jury what the conditions are in which you go through in order to verify that certain documents are, in fact, on the different devices that you've talked about?
A. It was different for each of the different -- it was a variety of devices and a variety of different types of files.
02:50 In they were in active space and an MD5 was available, as we spoke earlier, we would do that MD5 match to verify that that was there. If they were carved in recovered space, we would sit and go file by file and do a visual as we did like in the DjVu files. So there was -- we used a different -- a variety of different information to verify the information that was on

the exhibits.
Q. And is this the kind of activity that you can do on the fly when -- during cross-examination?
MR. FICK: Objection.
THE COURT: Sustained.
BY MR. CHAKRAVARTY:
Q. What are the circumstances -- what are the resources you have at your disposal to do that?
A. Well, we have the forensic team here in Boston, and we
02:50 were -- I mean, the process to validate and verify took days to do, 20-hour days, probably four, five days of looking through every single one of the files on the exhibits. And this was just a subset of the totality of all the files that were seized in the case or that were a part of the forensic process in the case.
Q. In response to one of the questions from Mr. Fick you said that it's -- you weren't sure what one of the files on one of the -- I think the file system record date was. Is that right?
A. I was actually not sure of where that information actually
02:51 originated from.
Q. Right. And at one point did you know that and just didn't remember?
A. Again, we used a variety of different tools to verify that information.
Q. Can I show you something that might refresh your

recollection?
A. Okay.
MR. CHAKRAVARTY: May I approach, your Honor?
THE COURT: You may.
MR. FICK: Can I ask to see what he's showing the witness?
THE COURT: Show it to Mr. Fick.
(Pause.)
BY MR. CHAKRAVARTY:
02:52 Q. I'm handing you a note. Can you read that to yourself, please?
A. Okay.
Q. Does that help refresh your recollection?
A. It puts the information in context.
Q. All right. And is that just a note?
A. It's just a handwritten note.
Q. What I've just handed you is a handwritten note?
A. Yes.
Q. With that information could you explain what the file
02:52 system record date was that was in that column?
A. The record column was the column, as we had spoken about, was created by AD Labs, or was taken from AD Labs.
Q. And is that your memory that you're testifying from?
A. Yes.
Q. And so various tools -- different tools were used at

different times in order to both extract data as well as to verify data. Is that fair to say?
A. Yes.
Q. And if you used two different tools to do the same function, does it sometimes produce different results?
A. It depends on where it's pulling that information from.
Q. So if you're comparing data from one tool with data from another tool, is that like comparing apples to oranges?
A. For the most part, yes. The tools are tested and
02:53 validated, although there are different version of the tools. And, again, I would have to go back to the original tool to get to the specific on that.
Q. Mr. Fick asked you about some of the activity that occurred on the Sony VAIO computer. And when you had extracted files from the Sony VAIO computer, did you make observations of other files that were on that computer other than the ones that you extracted?
A. I didn't extract the files; I just utilized the exhibits and went back to the original file set in the software and
02:54 determined that they were there.
Q. And were you able to make a determination as to who the user was of that Sony VAIO computer?
A. Based on the activity that we were preparing and verifying from the exhibits that -- you know, we determined that it was Jahar's laptop.

Q. And the fact that other devices were also plugged into that laptop, how did you come to that conclusion?
A. Well, again, as we had spoke about before, in the registry there is a report that will track all of the physical devices that are plugged in through the USB ports.
Q. So when Mr. Fick asked you as to whether some of the dates of the creation of some files on that laptop predated -- I think the date that he used was September 2011, does -- from the file listing, if the file listing was created -- or showed
02:55 that a file was created after September of 2011, could you conclude as to who the likely user of that laptop was for that file list?
A. I'm not sure. Can you rephrase the question?
Q. I'll rephrase. It was a bad question.

The complete file listing, did it show the dates that the files were accessed on that computer?
A. It would show a created/modified/accessed in the file record or born-on update.
Q. And you described that no good computer forensic scientist
02:55 would rely exclusively on the Windows information. Is that right?
A. There are a number of different pieces of information that we would draw on to make a determination.
Q. Okay. And could you explain just to the jury why just if they see a date, that's not dispositive as to when something

might be accessed?
A. Well, it depends -- when files are created, depending on where they're created, sometimes if they were created on the Internet and you put a thumb drive in a computer and download that file from the Internet to the thumb drive, it's never really born on the computer; it could have been created someplace else and then written to the thumb drive. So you would have to use a number of different pieces of information to determine the actual, you know, creation date on that
02:56 computer.
Q. And so the file that Mr. Fick showed you actually had a creation date of October 10th of 2011. Do you remember that?
A. Which file? He showed me --
Q. I think it was the Five Ground Rules. It was a very dense chart. It's not worth putting it back up on the screen, but it was a very dense chart that you had to zoom in on. Do you remember that?
A. Yes.
Q. And so October 10, 2011, in the complete file listing,
02:56 what does that mean?
A. What column was that --
Q. I think it was in the creation --
A. In the creation? With the X-Ways report, it would have been when that was created, or created on that computer.
Q. So that means during the school year of 2011, that file

was created on the Sony laptop?

MR. FICK: Objection.

THE COURT: Sustained.

BY MR. CHAKRAVARTY:

Q. What does that tell you about the -- in relation to the school year as to when that file was created on the Sony laptop?

MR. FICK: Objection.

THE COURT: Sustained.

02:57 BY MR. CHAKRAVARTY:

Q. Can you conclude anything about the creation date of that file on that computer?

A. Other than the report shows that it was that date of October 11th.

MR. CHAKRAVARTY: Call up 1143-01.

Q. This was a document that Mr. Fick showed you.

MR. CHAKRAVARTY: Can we go down to the last page, or two pages down, please? Keep going down to -- I think it's January 1st. Keep going. Right there.

02:58 Q. So he highlighted this entry where the JTsarnaev Yahoo mail account was accessed. Is that right? Do you remember that?

A. Yes.

MR. CHAKRAVARTY: And so if we can go back to the earlier page, Mr. Bruemmer.

Q. Just to clarify, this spreadsheet was generated from the desktop computer that was at the residence of 410 Norfolk Street. Is that right?

A. Can you go back up to the top of the report, please?

MR. CHAKRAVARTY: Page 1, please.

A. At 2R14. Yes, the HP desktop.

Q. So this showed that somebody logged into the JTsarnaev Yahoo email account on that computer on January 6th?

A. There was a browser history record on that computer of somebody logging into that email account.

Q. And Mr. Fick also asked you about when Tamerlan Tsarnaev was not in the country, and he gave you like a six-month period through July of 2012. Do you remember that?

A. He asked that question, yeah.

Q. And so all these dates that occurred before July of 2012, that would suggest that it was somebody else using this computer. Is that fair to say?

MR. FICK: Objection. Those aren't the dates on the screen. The dates on the screen are 2013 dates. Oh, I'm sorry. I'm on the wrong screen.

THE COURT: All right. Go ahead.

BY MR. CHAKRAVARTY:

Q. Sir, you can answer the question. The question was: Does it mean that the user of this computer was not Tamerlan Tsarnaev during that time?

A. It was not Tamerlan Tsarnaev.
Q. So all of this ESPN, MTV, all that stuff was not Tamerlan Tsarnaev, right?
A. It was not.
Q. Okay.
MR. CHAKRAVARTY: Can we go to the next page?
Q. And that goes on for another page.
MR. CHAKRAVARTY: Go down to the next page.
Q. And another page. It looks like somebody's watching "Teen Wolf."
MR. CHAKRAVARTY: Next page.
Q. And Netflix as well, and then "Walking Dead." These are all things that that person liked to watch?
A. That was the Internet access that was recorded during that time.
MR. CHAKRAVARTY: Now can we go to the file listing of 1143?
Q. So going back to 1143, we called up one of the folder directories. These are some of the files that were on the 1143, the desktop computer in the Norfolk Street residence, right?
A. Except for the ones that are denoted with an A, they're actually the translations for the files that correspond to the numbers.
Q. So all of the "Hereafter Series" is in there from Anwar

Awlaki. Is that right?
A. Yes, they are in that folder.
Q. And a number of audio files, or nasheeds. Is that right?
A. Can you scroll over for a second?
Q. In fact, some of these nasheeds were also found on the 1R6. Is that fair to say?
A. I would have to look at the verification, but I recognize some of the titles from --
Q. Some of the titles. But until you see an MD5#, you
03:01 wouldn't be able to --
A. No.
Q. And there's some videos as well?
A. That came out of the new folder, yes.
MR. FICK: Object to the scope at this point.
THE COURT: All right.
MR. CHAKRAVARTY: I'm done with this.
THE COURT: All right.
BY MR. CHAKRAVARTY:
Q. Now, you were also asked about whether there were any
03:02 other computers in the Tsarnaev family household prior to this desktop computer that -- whether you were aware of any other computers. Do you remember that?
A. Yes, I was asked that question, yes.
Q. And going to 1557, we haven't talked much about the 2R58. Do you see that?

A. Yes.
Q. What do you know about that device?
A. Well, from the description --
MR. FICK: Object to the scope.
THE COURT: Sustained.
BY MR. CHAKRAVARTY:
Q. Were there other devices found in 410 Norfolk Street?
A. There are other devices on this list that were found from 410 Norfolk Street.
03:03 Q. And with regard to the data that is on the disks that you've entered into evidence, with the exception of those pieces such as translations and the derivative analytical products which have some titles and things on them, was everything else that you brought into court actually found on each of the devices that you have talked about?
A. With the exceptions that we spoke about this morning with the titles of the corrupted files and the DjVu files that were converted, yes.
MR. CHAKRAVARTY: That's all I have, your Honor.
03:03 MR. FICK: Very briefly. Just one moment.
(Pause.)
MR. FICK: Could we have the screen back to the monitor here?
THE COURT: I'm waiting for something to come up.
MR. FICK: Okay. Is this the cord that's attached,

because it should be --

THE COURT: No, I have it. I'm just waiting to see whether there's an image and then I'll expose it.

MR. FICK: Oh, I see.

(Pause.)

RECROSS-EXAMINATION

BY MR. FICK:

Q. Now, Mr. Chakravarty asked you some questions to clarify -- or at least try to clarify the meaning of this file -- system record date in local time, right?

A. Yes.

Q. He showed you something on a handwritten piece of paper. Who wrote that?

A. I don't recognize the handwriting on that.

Q. So anyway, your answer to the question was the data from the second column came from the AD Labs tool, right?

A. I said the record column is in AD Labs. That's what all that --

Q. All right. But regardless of what tool we're talking about, all of these tools extract information from the -- from Windows and from the Windows metadata, correct?

A. They do. But they also could interpret it in different ways.

Q. But ultimately there is an answer, for example, to the question about when a file was created on a local computer,

right?
A. There's information available from numerous sources that were used to determine when that file was created on that computer.
Q. And if tools conflict, one would have to look deeper to figure out what the conflict is and answer the question, right?
A. They would have to do some additional analysis to determine that.
Q. Now, quite apart from what tool generated this file system record date, my question is still which Windows artifact is the file system record date?
A. I'd have to check with AD Labs. I don't have that information sitting here today.
Q. Okay. So even if now you remember from the handwritten note that AD Labs generated this information, you still can't tell me what that information means?
A. Not without having the software in front of me, no.
Q. Okay.
MR. FICK: That's all.
THE COURT: All right, Agent. Thank you. You may step down.
THE WITNESS: Thank you.
(The witness is excused.)
* * *

C E R T I F I C A T E

We, Marcia G. Patrisso, RMR, CRR, and Cheryl Dahlstrom, RMR, CRR, Official Reporters of the United States District Court, do hereby certify that the foregoing transcript constitutes, to the best of our skill and ability, a true and accurate transcription of our stenotype notes taken in the matter of Criminal Action No. 13-10200-GAO, United States of America v. Dzhokhar A. Tsarnaev.

/s/ Marcia G. Patrisso
MARCIA G. PATRISSO, RMR, CRR
Official Court Reporter

/s/ Cheryl Dahlstrom
CHERYL DAHLSTROM, RMR, CRR

Date: 3/25/15