UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	Criminal Action
v.	)	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

JURY TRIAL - DAY THIRTY-SIX

Testimony of Kevin Swindon

John J. Moakley United States Courthouse
Courtroom No. 9
One Courthouse Way
Boston, Massachusetts 02210
Thursday, March 19, 2015

Cheryl Dahlstrom, RMR, CRR
Official Court Reporter
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
On Behalf of the Government

FEDERAL PUBLIC DEFENDER OFFICE
By: Miriam Conrad, Timothy Watkins, and
William Fick,
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

(EXCERPT AS FOLLOWS:

MR. CHAKRAVARTY: Supervisory Special Agent Kevin Swindon.

THE CLERK: Sir, you want to step up to the box, please.

KEVIN SWINDON, Sworn

THE CLERK: State your name. Spell your last name for the record. Keep your voice up and speak into the mic so everyone can hear you.

11:41 THE WITNESS: Thank you. First name is Kevin. Last name is Swindon, S-w-i-n-d-o-n.

DIRECT EXAMINATION BY MR. CHAKRAVARTY:

Q. Good morning.

A. Good morning.

Q. Where do you work?

A. I work for the Federal Bureau of Investigations.

Q. In what capacity?

A. The supervisory special agent for the Cyber Squad in the Boston division.

11:41 Q. What does the Cyber Squad do?

A. The Cyber Squad is responsible for investigating cyber matters in Maine, New Hampshire, Rhode Island, and Massachusetts as it relates to computer intrusion matters for criminal and national security.

Q. Do you supervise any other units or squads?

A. I do. In our program -- I'm here in Boston. We also have the Computer Forensic Analysis Team, or CART. And, lastly, we have the photo program, which is also under the Cyber Squad here in Boston.
Q. What does the Computer Analysis Recovery Team do?
A. The Computer Analysis Response Team is responsible --
Q. Response.
A. -- for the imaging and processing of digital media for all the investigative responsibilities for the FBI.
11:42 Q. How long have you been a special agent?
A. I've been a special agent a little over 18 years.
Q. Have you had particularized training in computer forensics?
A. I have. Prior to being the supervisor of the program, I was a certified forensic examiner for ten years.
Q. What is a forensic examiner?
A. A certified forensic examiner in the Bureau is an employee who's trained and responsible for the collection and processing of digital media for all types of investigations.
11:42 Q. You say "digital media." Can you give examples of what digital media is?
A. Sure. Digital media can be a thumb drive. Could be a computer. Could be a server. Could be anything where digital media would be housed or stored.
Q. Has that role of computer forensics increased over time?

A. Absolutely. It's increased a hundredfold over time. I think every investigative responsibility that the FBI has has seen an increase in digital media associated with it.
Q. Before you became a forensic examiner, did you have particular training in computer forensics?
A. I came out of the computer industry in the private sector before joining the FBI in 1996.
Q. And then in the FBI did you have any training?
A. We did. The certification for the forensic program is
11:43 intensive, requires an A+ and Net+ certifications. There's a two-week basic data recovery, a one-week advanced data recovery, practical exams, and then a moot court in order to be completely certified.
Q. You mentioned that you had been in the private industry as well. What was your job then?
A. My private industry job prior to the Bureau, I did network consulting to the hospitality industry.
Q. What's your education?
A. I have a bachelor in science and industrial management
11:44 from University of Lowell. I have a master's in business administration from Northeastern and a master's in finance from Boston College.
Q. Aside from your computer forensic certifications, have you had any other certifications in your career in computers?
A. In computers. The cyber training program, to be a cyber

agent, there are several phases of classes that you go through or that you progress through. And that was -- those classes were taken through -- there's four phases for a cyber special agent, and I completed the three of the four phases.

Q. You also stay up to date through your supervisory duties?

A. Yes. Supporting or managing the program requires a constant update of staying current with technology and aware of the current threats and trends in cyber.

Q. Are you active in InfraGard?

11:44 A. We have a full InfraGard chapter here in Boston, which is a public/private organization where the FBI partners with private sector to provide training and awareness on cyber threats and trends.

Q. Do you present on computer forensics?

A. I do. Typically have -- give presentations 15 to 20 probably per year on cyber-specific threats and trends and then several computer forensic presentations.

Q. Have you personally completed computer forensic examinations over your career?

11:45 A. I have.

Q. About how many?

A. In the -- to get an exact number would be very difficult, but it's over a couple of hundred.

Q. In addition, have you participated in and supervised others doing their forensic --

A. I have. I have been the program manager or the supervisor of the CART program for the time that I've been the supervisor in Boston.
Q. Over the course of that time, has there been peer review of your work and have you conducted peer review of others' work?
A. Yeah. As a part of the forensic process, there's a certain percentage of -- certain percentage of examinations that get peer reviewed and admin reviewed, and I've been both
11:46 -- I've participated in both processes.
Q. Have you testified previously as a computer expert in computer forensics?
A. I have. Yes, I have.
Q. Have you testified before Federal District Court in Massachusetts?
A. I have.
Q. And have you testified in other courts as well?
A. Yes.
Q. Have you done computer forensic analysis in terrorism
11:46 cases before?
A. Yes, I have.
Q. About how many times?
A. Probably four or five times specific to terrorism matters.
MR. CHAKRAVARTY: At this point, your Honor, I'd ask to qualify Agent Swindon as an expert in computer forensics.

MR. FICK: No objection.

THE COURT: All right.

Q. Agent Swindon, can you explain to the jury what computer forensics is?

A. Computer forensics has really evolved over the last number of years where previous -- as technology started to become what it is today, the process has changed. It's become more of a forensic science where there's a process and procedure for most things that we do including how we handle the evidence upon collection, what we do when we image it, and then how we process it. It sort of has become much more standardized over the course of time.

Q. And the forensics part of it, what are the primary objectives of conducting forensic analysis?

A. The primary focus would be to -- you know, to acquire evidence in a forensically sound way so as not to change that evidence but, in the process, being able to collect that evidence and make it usable in legal proceedings.

Q. What types of digital media are prone to computer forensic analysis?

A. We process a variety of different types of digital media. It can range from thumb drives or USB thumb drives to external hard drives, to laptops, to computers, to servers in businesses. Anything where digital media would be stored we have the -- we have the ability to process.

Q. Is there a general -- are there general phases of the computer forensic process?
A. There are general phases although each may differ slightly based on the type of media or the digital media that you're processing. But, typically, it's sort of a two-phase process where there's an imaging phase and then a processing phase.
Q. What is the imaging phase?
A. The imaging phase would be the process by which you acquire the initial image of that evidence. We would use either a piece of hardware or a piece of software to acquire a bit-by-bit image of -- or a forensic copy of that device or digital media.
Q. What types of techniques do you use to do that?
A. If it was a software technique, for example, if it was a hard drive, if it was your home computer, and we had to image that home computer, we would remove that hard drive from the computer, connect it to another computer in our lab with a -- the ability to write protect so as to not write back to that drive. And we would use a software application to image that drive.
Q. The software applications that you use in your computer forensics work, are those industry standard software applications?
A. They are commercially available, and most of the tools we use are commercially available.

Q. Are those used routinely by FBI offices around the country?
A. Yes. Forensic practitioners around the country would be utilizing those tools.
Q. Agent Swindon, you used the word "image." Can you explain what that means in the world of computer forensics?
A. Sure. Typically, there are two types of images we can make of a piece of digital media. There's going to be a logical copy and a physical image. The physical image is going to be a bit-by-bit copy of that piece of digital media. It's going to ignore the operating system. So whether it was, for example, an Apple computer or a Windows computer, that imaging process would ignore that operating system and then image that drive bit-by-bit.

The other alternative, if that's not available to do, would be a logical copy. For example, if you were on your home computer at home and you wanted to copy files off, you could go to your computer -- Windows computer and copy from your C drive over to another drive, would be a logical copy.
Q. So when you're talking about an image, you're not talking a photograph. You're talking about the content of the media?
A. The physical image would be an exact duplicate of what was on that drive at the time it was seized.
Q. When you say "bit-by-bit copy," you mean the little bits of data?

A. It goes down to the disk and, again, ignores the sort of operating system that's on that drive and would make a bit-by-bit copy.
Q. How do you verify that an image was done properly?
A. There are several techniques that you can do that, but the most widely accepted is going to be an MD5. I'll explain what that is. A MD5 is a technique that we use in forensic sciences to validate or verify that an image is made and collected properly or matches the drive that you're copying.
11:51 MD5 would be similar to like -- an MD5 value would be similar to say, like, a fingerprint. We would run a program against a folder, a file or a drive, and that program would generate that MD5 hash value. And that value would be unique to that file folder or drive. We then could compare that number, that unique number, to that file folder or drive at any point in time during the process to verify that no changes were made to that image or collection that we made.
Q. Is that routinely done when an image is made pursuant to the FBI's CART protocol?
11:52 A. Yeah. Most imaging software have it automated as a part of their process now. So when you do make that physical image, it would also calculate an MD5 hash value.
Q. You said that was the first phase of the computer forensics process?
A. Yes. Imaging is the first phase and, typically, the most

important phase.
Q. So what comes after the imaging phase?
A. After the imaging phase, depending on the investigation or the case and the request of the actual case agent who's in charge of the case, we would then process that image or process the data that we would have collected in their image form.
Q. What do you process that data with?
A. We -- typically it's commercially available software that we would process with. We would try that first. And then that
11:52 commercially available software would do a number of things. It would take a look at that image. It would look inside that image that we just made and be able to pull the data out of that image, for example, the documents, the spreadsheets, photos or images that might be on that drive. It would also give us access to other things on that drive that you may not see as a user, which would include deleted files or recovered files that you may think are deleted on the computer but are still recoverable by the forensic software.
Q. What are the tools that you typically use at the FBI?
11:53 A. Typically use -- we have a number of tools that have been tested and validated. Typically, the primary choice is going to be AD Labs, which is a product made by Forensic Toolkit or AccessData. And then, secondly, X-Ways Forensics has a new tool that's been provided in our toolkit of tools that have been tested and validated.

Q. So once you've processed the data that was imaged, can you make that available then for agents or other people to be able to look at that?
A. We do. Once it's processed, we have a -- for lack of a better term, a graphical user interface, that we would provide that processed image to a case agent or an analyst to be able to review. It would allow them to be able to look on that computer or look into that computer to see what files existed or look in that image.
11:54 Q. That would go for some of the other digital files that you mentioned earlier, like video files or pictures?
A. Sure, yes. The forensic software typically breaks them out and categorizes them by Word documents, Excel spreadsheets, PDFs, JPEG or images that might be on your computer.
Q. How does this differ from -- if the typical circumstance where a person might take a memory card out of their camera and plug it into their computer?
A. Well, what happens is when -- if you were to take that card out of your camera and put it into the computer, it would
11:55 actually make changes to that card. The forensic process, we would make sure that the way that we image that piece of media, there would be no changes made to it or the image upon collection.
Q. In addition to the pictures that may be in what we call active space, could you find other data on that card?

A. The software -- the forensic software has the ability to do several things. One of the tools it has, it can identify previously deleted files. So, for example, if you had a file on your computer that you deleted and it still existed or the data still existed on that drive, the application software would have the ability to identify that it had been deleted and then be able to recover that file and make it usable or visible to the person who's reviewing.

Q. Once that process is complete and the analysis of the data on a computer is complete, what's the next phase of the process?

A. What typically we would do is, based on the request, we would then provide that processed image to a either case agent or team or team of analysts or a team of investigators who would then review that data.

Q. And then, if that team then identified particular files that they wanted to extract from a particular computer device, how do you do that?

A. Typically, the investigative team or the reviewers would then -- they may -- if they were using AD Labs, which is a typical software we would use, they would make bookmarks or they would -- like bookmarks in -- if you were reading a book and put a bookmark to save your page, they have electronic bookmarks that they would mark data that we then, as a forensic examiner, then can go back into that software afterwards and

then export those files that they had identified as being significant.

Q. How do you export those files without changing the original data on the device?

A. Well, typically, we would then have the -- we would have the MD5 hash value for that file if it was a file of significance. And then we would -- just like you would burn a CD at home, we would burn that file to something or a piece of media that couldn't be written to again. Typically, like, we would use a CD-R which you could burn once. We would write those files to and then provide that to the investigative team as what we would call derivative evidence.

Q. Now, as a computer forensic examiner, would you select which files need to be exported?

A. In most cases probably not. It would -- we don't know the most about the cases. The investigators or the analysts know the most about the cases. We can assist them if it was a -- sort of a -- say it was a complex white collar crime, and the agent might be a white collar expert but not a technology expert. We may help them through the process of identifying where the evidence might be, but they're going to know best what evidence is most important to the case.

Q. What steps are taken -- you mentioned that there was an MD5 hash taken after an examination, is that right?

A. The MD5 hash is collected or first calculated at the point

of imaging.
Q. Okay. So you explained that that's a unique number. But what does an MD5 hash value go to? Is it a computer? Is it a file or what?
A. It can actually verify a file, a folder or a complete drive or an image. If you were to run that program or the program that generates the MD5 hash value for that file, folder or drive. You would then hold that, and that becomes a part of your admin file, your log file, so that way later you can
11:58 compare to make sure that no changes were made to that original evidence.
Q. The process that you just described of the imaging, the processing, the analysis, and the export of digital data from media, is that a standard process that the FBI uses?
A. It is. I mean, it's part of the forensic training for new examiners, or for examiners.
Q. Is that a process you've done as long as you've examined computers?
A. Yes.
11:59 Q. Now, let's draw your attention to this investigation, this case. Have you been working on the Boston Marathon investigation off and on over the last couple of years?
A. Yes, I have.
Q. At the beginning of the investigation, what was your role?
A. My role at the time, I was temporarily assigned as an

acting ASAC for the office for the cyber and counterintelligence branch.

Q. And so after the Boylston Street explosions, what was your duty?

A. Immediately following the Boston Marathon bombing event, I became responsible for overseeing the digital media collection and, operationally, sort of the day shift, if there really was one, in the command post.

Q. The digital media collection, what types of digital media were being collected?

12:00

A. There was a number -- again, there was a number of different types of media that were collected as a part of this investigation. There were cell phones and thumb drives and computers, DVRs such as the DVRs that were taken from Boylston Street, and a number of different types of evidence.

Q. At some point did your role change in the last two years?

A. It did. Operationally, once the person that I was acting for came back from their temporary duty assignment, I then -- I resumed my duties as the supervisor of the Cyber Squad in Boston.

12:00

Q. What was your role for purposes of testimony in this case?

A. For purposes of testimony in this case, I was asked by the investigative team to validate and verify those -- as we spoke about earlier, those sort of selected files that were made from those processed -- the processed pieces of evidence.

Q. Now, how many people have worked on the computer forensics process in this case?
A. Immediately following the bombing, we mobilized teams from a number of different offices, to include, New York, Philadelphia, and as far away as Miami, to come help support the collection or ingest the computer forensic evidence. So I would say, would estimate, there would have been over 50 different sort of certified forensic examiners that were involved in either collection or processing.
12:01 Q. And that's in addition to the people who actually seized items of evidence?
A. That is in addition.
Q. That is in addition to the people who actually analyzed the evidence?
A. Yes. It may be different, yes.
Q. Were there other agencies that participated in that process as well?
A. There were several task force agencies during the actual initial event that were assisting in the collection, the
12:02 collection of -- there were so many scenes that had to be processed, that we utilized some of the other agencies that provided assistance.
Q. And were all -- was all of the evidence that was collected by the FBI, the digital evidence, was it processed using the computer forensic process that you described earlier?

MR. FICK: Objection to foundation.

THE COURT: Overruled.

A. Yes. At both Black Falcon and One Center Plaza were the two sort of forensic collection points for digital media. They were staffed with fully certified forensic examiners who follow the same SOP, standard operating procedures, and guidelines.

Q. Were you supervising them at the time?

A. I oversaw the collection, yes.

Q. Did you go to Black Falcon? Did you go to the Center Plaza?

12:02

A. I did. I was assigned to Center Plaza, which the forensics lab is right next to, where the command post was set up and made daily visits over to Black Falcon to brief them on the events of what was going on.

Q. As part of the FBI's analysis protocol, were there steps to ensure that you have legal authority to actually search these devices?

A. Absolutely. All the evidence in this case was seized pursuant to legal authority.

12:03

Q. At Black Falcon, you've mentioned, is this the staging area where evidence was taken after the bombings?

A. Black Falcon was initiated to help -- have one place where evidence could be. There was -- evidence was so voluminous that we needed to find a place where we could bring in -- a large enough area to bring in all the evidence. And Black

Falcon was provided, I believe, by Massport to be the ingest for evidence, including the digital media.
Q. And can you explain a little bit how the computer forensics work was happening at Black Falcon?
A. We set up a lab at Black Falcon that mirrored the lab that we have that's permanent in One Center Plaza. We have a mobile sort of command post per se that came up from New York and has full access and full technology that we would have in a typical permanent lab, and they deployed -- they can deploy it in the
12:04 field.
Q. How was the computer forensic process happening at Center Plaza?
A. According to -- our forensic lab is a permanent lab. So, really, it was -- other than being busier, it was -- it was standard procedure for us there.
Q. Let's draw our attention to some particular devices in this case. About how many devices were seized in the course of the Boston Marathon investigation?
A. I believe at last count there were over 600 pieces of
12:04 digital media that were collected.
Q. Did you examine each one of those?
A. I did not examine each one of those.
Q. In fact, do you know if any one person has?
A. I do not believe one person has examined all 600 pieces of digital media -- or one single person, I'm sorry.

Q. Is it fair to say that, of the 600 devices, there were a variety of different types?
A. Yeah. There were numerous different types, as we described before, whether it be phones, thumb drives, computers, laptops, digital video recorders from businesses.
Q. Would the data on those devices amount to, you know, megabytes and gigabytes and terabytes worth of data?
A. Yeah, there were terabytes of data.
Q. Were you asked to look at some specific devices in this case?
A. I was. As a part of the process, as we described earlier, there was an imaging, a processing, and then a team views or exhaustively searches the processed material. Once they've identified the files or items of interest, I was then asked to validate and verify that those items of interest existed on the pieces of evidence where they originated from.
Q. When you say "pieces of evidence," on the devices that were seized by the FBI?
A. On the devices, right, that were associated with the investigation -- on the number of different investigations, yes.
Q. You were confirming what material -- some of the materials that were on those devices?
A. Yes.
Q. And how did you do that?

A. There was a set of disks that we have, and those disks had evidence files that were numbered. And based on a numbering system of an exhibit number, the files were then, to the best of their ability, kept the true name. They were then compared to files on the computer of where they originated from.
Q. And how did you compare it with the files from the original computer device that was seized?
A. We went back into -- when we talked about earlier, the forensic software called AD Labs, which is where the evidence or the images of those evidence were staged. We went back in -- or I went back in with the CDs, went into AD Labs, and validated and verified that that -- that those files existed.
Q. How did you know which computers they were associated with?
A. The files were labeled where the images or where -- the files were labeled of what piece of evidence, where they came from.
Q. Is that pursuant to the standard imaging process that you described earlier?
A. Well, the numbering system is typically established with our Evidence Response Team.
MR. FICK: Objection. I don't understand the question.
THE COURT: Why don't you reask it.
Q. I'll reask the question. How did you know what devices

the files were from?
A. It was identified -- there's a numbering system that exists, and we cross-referenced the numbering system for the exhibit numbers to the evidence numbers that -- as we heard earlier, the Evidence Response Team numbers things on scenes -- at scenes.
Q. As a computer analyst, do you -- are you generally familiar with where pieces of evidence were found?
A. Typically. I mean, typically, because we would have to review the documentation before an exam proceeded. We'd need to make sure that legal authority was in proper order. We would need to know the locations of where things were from. We would need to know the background of that before the exam began.
Q. That's part of the standard practice?
A. That's part of the standard practice.
Q. As you verified the contents of these CDs, did you create something that would help explain your testimony?
A. We did. The number of pieces of evidence were so voluminous and the number of files that we're asked to validate and verify, we created sort of a spreadsheet to be able to recall what pieces of evidence that we would be talking about today.
MR. CHAKRAVARTY: I'd ask for the witness, 1153. Excuse me. Sorry. 1557. Excuse me.

Q. Agent Swindon, do you recognize this?
A. I do.
Q. What is it?
A. That is the spreadsheet that we made when we were first asked to start to validate and verify this process. It was a spreadsheet that we put together to be able to track what pieces of evidence we were using, and it gave us a snapshot of a quick reference.
Q. Would this be helpful in presenting your testimony today?
12:09 A. Tremendously, yes.
MR. CHAKRAVARTY: Your Honor, I'd ask that 1557 be marked as a chalk.
MR. FICK: No objection to the chalk except that I'd like him to clarify when he says "we" prepared this exhibit. Who's "we"?
Q. Who did you work with to prepare this exhibit?
A. No one. I created it.
THE COURT: I'll expose it.
MR. CHAKRAVARTY: Thank you, your Honor.
12:10 Q. Agent Swindon, can you read that?
A. I can, yes.
Q. How did you select these particular devices to make this chart about?
A. I didn't actually select the devices. These devices corresponded to the files that I was asked to validate and

verify.
Q. And so this is the universe of the devices that you looked at?
A. Yes, sir.
Q. Now, with the exception of a couple of these devices, did you actually go in and check file by file whether files that are going to be presented to the jury were, in fact, on these devices?
A. I was provided these CDs for the exhibit numbers and verified that the files existed on the pieces of evidence that are listed on the sheet here.
MR. CHAKRAVARTY: If I may approach, your Honor?
THE COURT: All right.
Q. Handing you a binder, Agent Swindon, do you recognize that?
A. I do.
Q. What is it?
A. It's a two-inch, three-ring binder, with two CD placeholders in it.
Q. Are there several CDs in there?
A. There are. There are 13 total CDs.
Q. Do you know what those CDs are?
A. I do. These are the CDs I was provided with to be able to check the files to make sure that these files that are on these CDs existed on these pieces of evidence.

Q. Did you, in fact, verify that?
A. I did.
THE COURT: What was the number of CDs?
THE WITNESS: Sorry. There are 13, sir.
Q. And, specifically, if I may, Agent Swindon, I'm going to read off a list of numbers on the CDs, exhibit numbers, and ask if you can verify that those CDs are in there.
A. Okay.
Q. 1141?
12:12 A. Yes.
Q. 1142?
A. Yes.
Q. 1143?
A. Yes.
Q. 1144?
A. Yes.
Q. 1145?
A. Yes.
Q. 1146?
12:12 A. Yes.
Q. 1147?
A. Yes.
Q. 1148?
A. Yes.
Q. 1149?

A. Yes.
Q. 1150?
A. Yup.
Q. And 1151?
A. Yes.
Q. Is there also an 1152 in there?
A. Yes, sir.
Q. Sorry. There's one more. 1457?
A. No.
12:13 Q. 1457 is not in there?
A. No, it is not.
Q. Okay. I'll have to get that.

With regards to 1141 through 1151, do those contain documents that were on each of the devices that they correspond to?

MR. FICK: Objection. May we approach?

THE COURT: All right.

(SIDEBAR CONFERENCE AS FOLLOWS:

MR. FICK: The objection is he's asking the question
12:13 based on a false premise. These CDs contain not only files from the various devices but various analytic spreadsheets of the -- either the FBI's or the U.S. Attorney's Office's own making. So it's, like, to ask the question in that form is itself misleading. And it sort of raises again the notice problem we had because these are the new disks we got yesterday

that now have different contents than what we thought they had before.

MR. CHAKRAVARTY: I'll certainly clarify that there are analytical files or metadata that's also put on there that he will explain, and he will go through each of the CDs explaining which ones correspond to which devices.

MS. CONRAD: But are you offering the entire disks?

MR. CHAKRAVARTY: I am going to offer the entire disks, not at this time.

12:14 MR. FICK: When the time comes, we'll deal with the issue.

. . . END OF SIDEBAR CONFERENCE.)

Q. Agent Swindon, do these CDs have the data extracted from the -- each of the devices that they correspond to?

A. Do the numbered CDs have the data extracted from the numbers of the -- corresponding to the pieces of evidence on the spreadsheet?

Q. Correct.

A. Yes, they do.

12:15 Q. Does it have all of the data for each of the devices?

A. It does not have all of the data for each of the devices. The data for each of the devices would be too voluminous to fit on this many CDs or DVDs, so it was -- a sample or particular files were identified by the team and then extracted and put onto these CDs or DVDs.

Q. Is it fair to say there are thousands and thousands of files on those computers?
A. There are.
Q. So can you explain what this -- sorry.
In addition to the files that were actually extracted and put onto these computers -- excuse me, the CDs, were there any other types of metadata or other files that were also put onto these CDs?
A. There are other files on the CDs. The other files would include a directory file listing for each of the devices when they could -- when they're appropriate or could be made. And then there are some derivative reports or derivative spreadsheets made from the data on that also.
Q. Okay. So what is a directory file listing?
A. A directory file listing would be a listing of all of the files that would exist on that computer.
Q. And what are the derivative spreadsheets?
A. A derivative spreadsheet would be a spreadsheet that would be created by someone that maybe aggregated information from several different places, maybe from the directory listing or maybe from other files on the computer for the ease of understanding.
Q. Can you give an example of a derivative file listing?
A. If -- for example, if you had a file listing for your whole computer or your whole computer at home, most of it would

be useless because you've got your Windows directory there with files that you don't need to see. But if you wanted a directory listing of just your documents and settings, you could do a full directory listing for your whole hard drive and then only select what you may want to see in your documents and settings. Gives you a snapshot of a smaller subset of what was on that computer.

Q. Are you familiar with internet history?

A. I am familiar with internet history.

12:17 Q. How is internet history exported from a computer?

A. Internet history resides on your computer, typically your browser, whether you're using either Mozilla or Internet Explorer or Chrome, would track a history of you being online or an internet history file where that history would reside. You can do a couple things. You could export that file individually to look inside of it, or there are other applications that we would use post processing to assist us in trying to look at that file and make it understandable and usable.

12:18 Q. Can you pare that down so you're only exporting some of the internet history?

A. Once you have access to that internet history file, you can either select a range of dates or you can select maybe a particular type of web page or URL that you were looking for and filter it by that.

Q. Were those derivative spreadsheets that you described, were those the result of that kind of a process?
A. In some cases on these CDs, yes.
Q. What other types of information were put on these CDs?
A. These represent several different types of media. So, for example, there are -- one of the CDs is from a couple of -- from iPhones that were collected as a part of the investigation. And they contain data on them that would -- from the SIM card on the cell phone. So a typical directory
12:19 structure, as we were discussing with a computer or a piece of media -- digital media, it would look differently on the disk.
Q. And what's a SIM card?
A. A SIM card is a card that would go into your cell phone that has a unique ID number which would allow you access to -- cellular networks would use it to authenticate your phone onto their networks.
Q. Let's go through the spreadsheet now and explain what each of the columns are.
A. The media was a description of the type of media that
12:19 piece of evidence was. The ID number was the ID number that was assigned typically by the Evidence Response Team appropriate to a search scene. A media description was a simple, short as we could keep it, description of what it was; the location where it came from. The "I" would be where it was imaged. The "P" would be where it was processed. And then we

did sort of a synopsis of the file types in that last column there.

Q. Let's start with the file types. Can you describe what those file types are?

A. Some of them are abbreviations. But the file type we'd -- the dir would be a directory listing. IH would be internet history. In the first line, iTunes would be -- or iTunes are a backup associated with an iTunes account. Audio or visual files; Adobe files; Word documents; or pictures.

12:20 Q. For the first one, it says over 500,000 total files. Is that how many --

A. We were trying to get the scope of how voluminous things were, and for particularly 1R6, it was over half a million files associated with that drive.

Q. The "P," is that what you said where the item was processed?

A. I'm sorry?

Q. What does the "P" stand for?

A. The "P" is where the items were processed.

12:21 Q. What does the "CP" --

A. "CP" would designate Center Plaza, which is where one of the forensics labs was located; and then "BF" was Black Falcon. And there were some items that actually went directly down to Quantico for processing, and that would be the -- designate the "QT."

Q. That appears down here where I'm circling?
A. Yes, sir.
Q. Center Plaza, incidentally, is that where the FBI headquarter office is in Boston?
A. One Center Plaza, Suite 600, in Boston, Mass.
Q. And the media, it says "C." What does that stand for?
A. "C" would stand for computer.
Q. What does "TD" stand for?
A. Would be thumb drive.
12:21 Q. What does "HD" stand for?
A. Hard drive.
Q. And CD?
A. CD-ROM.
Q. And "IPOD"?
A. IPods.
Q. And "cell"?
A. Would be cell phones or cellular telephones.
Q. And "GPS"?
A. GPS devices.
12:22 Q. With regards to the data that you got for this spreadsheet, was this data that was collected by the -- during the Boston Marathon investigation?
A. Yes. This was from -- what originated from a number of different locations. A chain-of-custody form would contain some of the pieces of information such as the description, the

location. The imaging and the processing information would have come from our CART reports. And the file types would have come from a review or a cursory view of what types of files were on that piece of media.

Q. Are you familiar with what a log file is?

A. I am.

Q. What is that?

A. A log file can be a number of different things, but typically a log file would be a clear text file that would have information in it that would provide a log of activity.

Q. Were log files maintained for these -- the devices as well or for some of them?

A. For some of them, yes.

Q. Were those put onto the CDs as well?

A. If they were available, they were put onto the CDs, yes.

Q. How familiar are you with each of these devices?

A. I'm -- most of the devices, I'm very familiar with because they correspond to a CD with files that were verified. There are several -- one was a -- done a cursory look, and there were several that were actually physically unable to be -- you know, to be processed. So it was just the SIM cards that were processed.

Q. Now, does computer forensics allow you to know whose computer some -- a computer device is?

MR. FICK: Objection.

THE COURT: Overruled. You may answer it.
A. There are certain limitations to computer forensics. As we've moved into -- computer forensics has moved into more of a forensic science, we rely on the data that we're able to collect to make determinations of access, determinations of files where they may reside. We also rely on the information that we get from the computer knowing, as we all know, our home computers aren't sometimes the most reliable. They don't always collect all pieces of information that we need. Some of
12:24 the things can be deleted either through user intervention or deleted automatically through program files or even wiped through applications that you could download on the internet. So we can only rely on what we have, you know, what we collect at the time when we collect it.
Q. So in your computer investigations, how do you know who owns a computer?
A. Typically, we would look at a number -- we'd start with a number of areas to look in the computer. When you first turn on your computer and register that computer, your name would be
12:24 captured, or if you did enter your user name, would be captured in the Window's registry file which is the file within Windows that stores all of the information about that computer, would be one way of identifying who potentially may be using or accessing that computer. In general, internet activity, you may be able to tell who is logging onto your email or an email,

who may be using social media or who may be using certain applications to do certain things.
Q. So you look at the content of what's on the computer to help figure that out?
A. We need to review the content to determine who would be utilizing it.
Q. In addition to the materials on the computer, do you do other investigations outside of the computer forensics in order to make those determinations?
12:25 A. Of course. The forensic examiner would provide as much information as he can to the investigative team who then may do additional interviews to determine usage.
Q. Is there any limit to how you can determine who was using a computer on a specific day?
A. I guess, barring having a computer over somebody's shoulder and filming them on the keyboard, there are limitations. We sometimes have to make assumptions, or based on internet activity we put together facts based on internet information and the technology.
12:25 Q. Is it true that sometimes you cannot say, to a degree of certainty, that you feel comfortable as to who was using a computer?
A. That's true, yes.
Q. Now, with regards to the devices in this case, can you testify regarding the content of those devices that you did not

examine or verify?
A. That are on this list?
Q. Yes, on this list or not.
A. Okay. The ones on the list -- the ones that we have CDs for, yes. The ones we do not have CDs for, where several of them there was a cursory look or check done and -- but as far as the scope of the media collected, the over 600, absolutely not.
Q. So on this spreadsheet, which of those that you did not do
12:26 that verification process for?
A. On D385, which is the third "C" down on the computer, the Samsung laptop from -- there was just a cursory look done of the directory structure.
Q. Are you aware whose computer that was associated with?
A. I believe, based on the location and other investigative information, that it was Tamerlan's computer.
Q. Was there another device that you did not do an in-depth look at?
A. It was the two cell phones that belonged to Azamat and
12:27 Dias were processed as a different investigation.
Q. Okay. Now --
A. I'm sorry. There's just one more. 1V1, the GPS 1V1, I did not process or look at that.
Q. Despite the fact that you didn't process or look at those devices, were those examined by the FBI?

A. All pieces of digital media were imaged, processed, and reviewed by somebody on the investigative team for the FBI.
Q. In fact, was there an army of analysts who were looking through these things?
A. You could define an army, but, yeah, it was a large team of investigators that looked at or culled through the evidence.
Q. Let's start with the 1R6. Does that correspond to the CD labeled Government's Exhibit 1142?
A. Yup, it does. 1142, yes.
12:28 Q. What computer does that CD contain data from?
A. That contains data from a Sony Vaio laptop that was collected at 69 Carriage Street that investigative, we believe, belonged to Jahar.
Q. The computer did?
A. The computer did, yes.
Q. Was that processed -- was that imaged at Black Falcon and processed at Center Plaza?
A. It was imaged at Black Falcon, yes, and processed at Center Plaza.
12:28 Q. And the CD that you have in front of you, does that contain files that were actually on that computer that were imaged near the time that they were seized and then exported onto that CD?
A. It contains files that were identified on that computer by the investigative team, written to the CD, and then verified

that they existed on 1R6 along with the other spreadsheets that we had discussed earlier.

MR. CHAKRAVARTY: At this time, your Honor, I'd move into evidence Exhibit 1142.

MR. FICK: Objection.

THE COURT: Let me see you at the side.

(SIDEBAR CONFERENCE AS FOLLOWS:

MR. FICK: So this is the contents, at least as of yesterday, of this exhibit, the disk exhibit here. These four directories contain the various files from inside the computer, as far as I can tell. These are the various derivative spreadsheets that somebody at the FBI, the U.S. Attorney's Office, I don't know who, created. And without a foundation, I don't see any basis to admit those things into evidence.

MR. CHAKRAVARTY: He's verified each of those spreadsheets. He didn't personally create them, but he knows what they are, and he knows how they were created. And he has verified that that content is on that computer.

MR. FICK: As I heard his testimony, he verified the files that were on the computer. He didn't say he verified the images.

THE COURT: Can I --

MR. FICK: Absolutely.

Whether or not he verified it, there's a question, a foundational question, of who made it, what procedures they

used to make it. If he doesn't know, I would suggest a huge confrontation clause, *Melendez-Diaz* and its progeny, problem about this kind of evidence.

MR. CHAKRAVARTY: First, he's an expert. He's allowed to provide hearsay for *Melendez-Diaz* purposes. But, more importantly, if he's confirmed that this is data that's on the computer in a variety of the different metadata exports that forensic software allows them, then that's his competence. That's what he is allowed to say.

12:31 MS. CONRAD: May I just --

THE COURT: How do I get back to the list?

MR. FICK: Just exit the --

THE COURT: Maybe just do that?

MR. FICK: Even if an expert can rely on hearsay, to put in the actual documents into evidence is another question entirely. You know, these are not -- the contents of the spreadsheets are not -- the spreadsheets themselves were not on the computer. What some human being has done is collected the information, put it in the spreadsheet, and presented it. It's

12:32 like a summary chart except the person who makes the summary chart ought to testify about how it was made and to verify that it's accurate.

THE COURT: Maybe. But I don't think necessarily if it's someone with knowledge of what it is and can say that's what it is.

MR. FICK: I think our ultimate position would be that all he's testified about now is verifying the files. There's no foundation there about the spreadsheets.

THE COURT: I agree with that. I think we need additional information about how those spreadsheets were prepared. I think it's likely that they will be submitted.

MR. FICK: We would maintain a confrontational *Melendez-Diaz* objection on top of the basic foundation issue.

That's actually a good suggestion Miss Conrad makes. The spreadsheets really ought to be a separate exhibit so that the jury doesn't get confused about what's from the computer and what's derivative. Right now, the way the government has done it is the disk has an exhibit number; the spreadsheets have a subnumber.

12:33

THE COURT: I think it can be made clear. It might be a better idea to have them separate. I don't think it's confusing for them to have --

MR. FICK: Please note the objection.

. . . END OF SIDEBAR CONFERENCE.)

12:33

THE COURT: That's 1142, I guess, right? 1142, is that it?

MR. CHAKRAVARTY: Yes, your Honor.

THE COURT: All right. That's admitted.

(Exhibit No. 1142 received into evidence.)

MR. CHAKRAVARTY: So, Mr. Bruemmer, if I could ask you

to open the display copy of 1142.

THE COURT: Is this all for everyone, right?

MR. CHAKRAVARTY: I think so. If it's admitted, then 1142 can be, your Honor.

Q. This first folder structure has identified just what device this was from?

A. Yes. That corresponds to the spreadsheet, yes.

Q. And so what is this?

A. This is the main root directory structure within that CD. The several files that are identified as where possible files were found on that computer in addition to there's a number of files there that were, as we talked about before, those derivative files that were created.

Q. The first four folders, is that what you meant that they correspond to the structure?

A. Actually, just Anzor files and public correspond.

Q. I'm sorry. What was Anzor?

A. I'm sorry. Anzor and public correspond files, and derivative derived Mobilsync do not.

THE COURT: I'm not following.

MR. CHAKRAVARTY: I'm not following either.

Q. Can you explain what the first four folders are?

A. There are four folders on that drive: one called Anzor; one called derived Mobilsync data; one called files; and one called public. Both Anzor and public existed on the drive in

that way or in that -- the way that it looks on the screen there. Mobilsync data and the files were added for organizational purposes on the CD.

Q. Okay. So were the contents of these folders actually on the 1R6 Sony Vaio computer?

A. The Anzor and the public, yes; the derived Mobilsync data has information in there that was derived from the Mobilsync backup on the computer. And then the files do have files that were derived from that -- from 1R6, yes.

12:36 MR. FICK: Object and ask to clarify whether he's talking about all or some.

Q. So can you explain whether you're talking about all of the contents of these folders was from the computer?

A. No. As we discussed earlier, the sum of everything is voluminous. This was strictly just selected files that were provided to me to verify and validate whether they existed on 1R6.

Q. Who provided you with the files that were of interest?

A. The investigative team did.

12:36 Q. So you said that there were, I think, derived files in the derived Mobilsync data folder and the files folder. What did you mean by that?

A. On 1R6, there existed Mobilsync backup files. Mobilsync backup files are associated with typically an Apple product. If you had an iPhone and you plugged your iPhone into your

computer and wanted to do a backup of it, it creates a backup file on that computer which would store a number of pieces of information including potentially contacts, information about the phone, your address list, your previous texts, your previous calls and your call log and images also from the phone.

Q. And the Anzor and the public folders, do those correspond to two different user accounts on the computer?

A. They do. I recognize those as being two different user accounts from the 1R6.

Q. And the files folder, what's in that?

A. The files folder was created for organizational purposes. Inside that files folder are other files from the drive.

Q. Okay. Then outside of each of those folders, there's a number -- there are a number of PDF files, with the exception of one text file, numbered 142-1 through 13 and 142-151. Can you explain what each of those are in turn?

A. Would you be able to bring those up one by one?

Q. Sure.

A. Thank you.

Q. This is 1142-01. What is this?

A. A little difficult to read on the screen. What this is this was an export of the internet activity that was identified on 1R6.

Q. And how is internet activity exported?

A. There are internet history files that exist on your computer. And a product -- a third-party product application was used for analysis called Internet Evidence Finder. It takes the internet history files and then puts them in a usable format. This here is a selection of the internet activity.
Q. And so is this a subset of all of the internet history that was exported using that software?
A. Yeah. I believe so, yes. I was given this file to determine whether or not these -- this internet history existed on the drive.
Q. And did you, in fact, confirm that?
A. We did.
Q. Is that through AD Labs, that software tool that you said earlier?
A. We used Internet Evidence Finder to parse out or to look into the internet history files.
Q. I'm sorry. Internet Evidence Finder, is that another commercially available tool?
A. Commercially available product, yes.
Q. Let's go to 1142-2. What is this?
A. This spreadsheet here is going to take a little bit of an explanation. This spreadsheet here is a snapshot of -- in Windows 7 and above, there are files on that computer called jump files or a jump list. A jump list is similar to what we would think of as a shortcut. When you create a shortcut on

your desktop or you create a shortcut for a file, Windows creates these things called jump lists. What jump lists track is a number of different things that happen when you open up a file. You need a third-party application like Internet Evidence Finder to be able to look into that jump-list file. But in there are several different artifacts, what you see here.

Q. So can you explain what these columns are and what information they tell you?

12:40 A. In the jump list, utilizing the parser software, we're able to see this -- typically, this report was provided as removable media or drives or anything associated -- it was associated with a D drive, which is typically an external drive or other than your C drive, which would be your hard drive on your computer. What happened -- this would be a designation of what information existed in the jump list for these dates and times for these files.

Q. Okay. When you say "external drive" and you talk about a "D" drive, what is -- explain how the computer assigns it the

12:41 letter D.

A. What happens in Windows is it's your first -- typically, your hard drive on your computer is a C drive. That becomes your initial -- or your drive where your operating system is stored. If you don't have a CD-ROM or a DVD or those are not designated, what will happen is Windows then goes to the next

letter to designate the next drive that you put in that computer.

So if you only had your C drive on your computer and you took a thumb drive or some external hard drive and plugged it into your computer, in order for Windows to access it, it needs to give it a drive letter. It would give the next drive letter available, and in this case, it was -- it would have been the D.

Q. And so does this spreadsheet indicate when devices were plugged into this computer?

MR. FICK: Objection.

THE COURT: Overruled.

A. The jump-start file, the jump-start information, has a bunch of information within it -- encapsulated within that jump list. In there could be when the creation date or when that first device or when that date and time of when that first file was created on that computer or viewed on that computer.

Q. When you say "could be," why do you say "could"?

A. There's a lot of variables based on time -- your date and time on your computer may not be completely in sync with the date and time that we're looking at right now here in the courtroom or maybe there's some other reason why it didn't collect the date and time when it was inserted into the computer.

Q. The volume label and the volume serial number, what are

those?
A. The volume label is typically associated with the device itself. It may designate the device. The volume serial number is the unique ID that Windows would give it in order to access the -- make the drive accessible within Windows.
Q. And some of these, they don't have a name. Is there a reason for that?
A. Yeah. Other than I recognize those directory structures as being associated with a camera, I don't know why there's a
12:43 volume -- not a volume label there.
Q. And the word "Patriot" -- the words "Patriot" and "Kingston," what do those means?
A. In this investigation or in this spreadsheet here?
Q. In the spreadsheet.
A. In the spreadsheet, they would be associated with the name of a thumb drive.
Q. Can you --
A. Or the manufacturer of a thumb drive.
Q. Can you explain local path, what this content is in that
12:43 column?
A. Typically, in the local path -- what this would show is that this volume label or this Patriot, this device that was named Patriot, was plugged into this -- you scrolled up on me there.
Q. Sorry.

A. This YouTube video, this word, Rasool Allah, *Inspiring Words of Truth*, video was accessed on this computer, and then Windows created this jump list which then collected this information.

Q. Looking at the last two entries, can you interpret what this -- the last -- the second -- the penultimate entry indicates based on this spreadsheet?

A. The last two entries appear to be link files, exclusively link files, which show that the D drive -- or if we're looking at the second one from the bottom, again, then the Patriot volume label had a file on there called completeinspire.pdf with that volume and was accessed at that date and time.

Q. For the *Complete Inspire*, it says January 21, 2012?

A. Yes.

Q. And what's the next file?

A. It says, "jointhecaravan.pdf."

Q. Does that say it was created on January 28, 2013?

A. Yes, it does.

Q. And last accessed March 15, 2013?

A. If you can scroll up to the top column?

Yes. That typically would be the last time that that file potentially could have been accessed.

Q. Now, in the course of your --

A. I'm sorry. Accessed on that computer.

Q. On this computer. On the --

A. Thumb drive -- if that thumb drive went to another computer, that last access time of that file is not going to match that last access time on that computer.
Q. So this spreadsheet only reflects data on the defendant's computer?
MR. FICK: Objection to the leading.
THE COURT: Overruled.
A. This information was taken from 1R6, yes.
Q. And not from that thumb drive?
12:45 A. It was not taken from the thumb drive, no.
Q. Go to the next one, 1142-03. What are these?
A. If this were two images that were exported from 1R6, probably the most important part to figure out where it came from is if you look at the path. It's a long string of a naming convention. But most importantly, from the root, if we take it four in from the root and start with users, that was the user's folder on the drive. Anzor was the user. And the documents and web cam, web cam media, capture, and it was an image.2.jpeg.
12:46 Q. Mr. Swindon, I think you just discovered it on your own, but if you want to annotate something on the screen, please just touch the screen.
A. I did that. Sorry about that.
Q. Were these all of the photos that were on the computer?
A. Those were not all of the photos on the computer.

Q. Like the other items, were they selected by the investigative team?
A. Selected by the investigative team.
Q. 1142-06, what is this?
A. As we talked about for 01, this is an internet activity report derived from Internet Evidence Finder on -- from the Sony 1R6.
Q. And so is this all of the internet history in the computer?
12:47 A. That is not all of the internet history. I believe there were over 30,000 entries across a number of different browsers on 1R6, and this was a subset of that information.
Q. And some of these entries have a date, and then some of them do not. What explains that?
A. That -- typically, what may happen is in some cases the internet history would grab a date and timestamp along with it depending on the product or depending on the browser itself, you know, whether it be -- again, Mozilla, Chrome or internet are the three sort of major ones. They all handle that
12:48 internet history potentially differently. So there may not be a date and time associated with an internet history entry that you see here.
Q. And all of this data on this spreadsheet, like the others, is this exported using the tools that you were describing earlier?

A. Exported using Internet Evidence Finder, yes.
Q. The dates and times on this spreadsheet and on the other spreadsheets related to internet history, how do you know whether those are accurate with regards to Eastern Standard Time?
A. Those are collected by the browser, and those would correspond to the date and time on the computer.
Q. So whatever the computer time was affects that?
A. Typically, yes.
12:48 Q. What is this next file, 1142-08?
A. As we had discussed earlier, a log is made when the imaging process is done for that piece of evidence. So this was -- this is the log entry for a device that we would call a TD3. That's an external standalone device that we would use to image the drive. It tells you the start/stop time and then what examiner created that image. And then down the bottom, as we mentioned, you'll see the MD5 hash value as we talked about earlier.
Q. So this reflects also the type of computer hard drive?
12:49 A. It does. It collects the hardware information about the actual hard drive that's in the computer.
Q. How big was the hard drive on the defendant's computer?
A. That drive, it's -- according to the TD report, is 500 gigabytes.
Q. What's the next file, 1142-09?

A. This file here is representative of the installed software that existed on the computer at the time it was imaged. This information is derived from the registry file. Windows has a registry file, which is typically the index for the computer. It stores information such as your user names, passwords, last accesses, different drives that had been connected to the computer. And it also includes a list of the installed computer.

Q. Does the registry file also serve as sort of a table of contents for the computer?

A. Not for the files on the computer within the directory structure, but what it does is it keeps all of the user information stored for the computer.

Q. Okay. Thank you. Is there a way that a computer keeps a table of contents?

A. I'm not sure I understand.

Q. Are you familiar with a master file table?

A. Yeah. Master file table is -- so the directory listing for the computer is basically your table of contents for human interaction. But the computer needs to be able to figure out where all those files are and translate that into the computer world of where it needs to access that on the disk. And the master file table would be where that information is stored. If you go to the directory structure to select a file, it would then point it to the master file table where it would find it

on the hard drive.
Q. If a file is deleted, what does that mean for the master file table?
A. When a file is deleted, there's a character that's changed, and it is no longer seen or visible to the user, but the entry may still be available in the master file table, and the data may still exist on the drive.
Q. If something has been deleted and then that space has been reclaimed by the computer, what happens to that data?
12:51 A. The data would be overwritten, and it would not be able to be recovered.
Q. I'm going to 1142-10. What is this?
A. This file is also out of the registry. It's the -- or the SAM file, which is the Security Accounts Manager. And this is going to list all of the users on the computer. As you can see, it shows administrator, guest account. And if you scroll down, these are all the users that were on that computer.
Q. So here it says, on the second page, user name, Anzor; full name, Jahar?
12:52 A. Yes.
Q. What does that mean?
A. That Anzor would have been a user on the laptop, on 1R6.
Q. Is that one of the folders that was -- one of the user folders that was exported in contents from that user profile?
A. Anzor was, yes.

Q. The -- does this show the last login date under the user name, Anzor; full name, Jahar?
A. It does.
Q. When was that?
A. The last login was Thursday, April 18th at 025.
Q. That's 2013?
A. 2013. But the designated Z is Zulu time. I believe, with daylight savings, minus 4, I believe is what it is.
Q. So it was last accessed, according to this data, sometime on Wednesday evening, April 17th?
12:53
A. Yes.
Q. 1142-11, what is this?
A. Again, out of the registry, this is the -- this shows that there's a valid Windows license on the computer; who the owner of the computer was based on the user; and then the product ID; and the product key for Windows.
Q. 1142-12, what is this?
A. This was a derivative report of selected link files, are those -- as we talked about before, the shortcut files from the computer.
12:53
Q. So explain a little bit more about what a link file is.
A. Link file is a shortcut or the Windows creates a shortcut. If you were -- for example, one way a link file would be created is if you were -- created a shortcut on your desktop, it would create a link file. Sometimes when you open files, it

creates -- automatically creates link files. So this would be a Windows-generated file that would be created.
Q. Does a link file get created every time somebody opens a file on their computer?
A. I haven't tested every piece of software that's out there, so I'm not sure how that would operate in the Windows 7 environment. I can't be for certain that every single software application that exists creates a link file.
Q. What are some circumstances in which a link file might not
12:54 be maintained by the computer when you export the file activity?
A. Well, there could be several reasons. One of the reasons may be a user could go in and actually delete a link file. If they were technically savvy enough to know where to find them, they could go in and delete the link file. Also, some programs create or keep a last-access list or a most-recently-used list. And it typically would hold maybe the ten last accesses or ten last access -- files accessed. And those are going to be sort of first in, first out, last -- yeah, first in, first out.
12:55 Q. And so the list here as -12, what can this tell you, as a computer forensics analyst, with regards to what usage was made of this computer?
A. Well, evaluating the report, I was asked to make sure that these link files existed on the computer. We validated or verified that they did exist on the computer, existed on 1R6.

If you're asking me to assess what this report is, I can look and say, from the information that's on here, at some point in time, these files were opened or accessed on this computer.

Q. This is 1142-13. What is this?

A. This is a spreadsheet that is a direct -- or a listing of the files and directories that existed in the user Anzor, a selected group of files -- folders that were in the user Anzor.

Q. When you say "the user Anzor," what does that mean?

A. If we go back -- reference back to the registry file that we had, it shows that Anzor was a user of the computer. So when they -- whoever established -- originally established the computer, which it says Anzor and Jahar, whoever established that user name decided to call that user name Anzor. And then Windows will create a folder called Anzor to store the documents, the photos, the videos that were associated with that user.

Q. So that's a user-defined field? It's not automatic?

A. It is a user-defined field although the operating system creates it.

Q. So there are more files here than appeared on the file-access spreadsheet with the link files. Does that mean that these files weren't accessed?

A. This list here is a list of the files that existed -- or selective list of the files that existed within that user Anzor.

Q. What can you say about whether these files were accessed?
A. I would have to look. If you can scroll to the right a little, there's actually -- in this particular spreadsheet here, access time is not -- the last access is not -- I'm sorry. The last time the file was modified is not listed in there. This is a directory listing of the files that existed in the user Anzor.
Q. In computer forensics, how do your determine whether and when certain files were accessed?
12:58 A. We would have to look -- we could look in the link or the shortcuts. We could look in the registry. There's a number of different places we could determine whether or not a file was opened.
Q. Are those exhaustive?
A. Yeah. The searches are exhaustive, yeah.
Q. The searches are exhaustive. Can you tell definitely whether a file was accessed?
A. In some cases, you may not be able to. You could see when it was created on the computer, but you may or may not have
12:58 record of the last time that that file was accessed.
Q. You can only testify to what you have a record of; is that fair to say?
A. I can testify, yes, what the data that we collected on the computer.
Q. What's 1142-51?

A. 1142-51 is the file listing for the entire computer.
Q. Okay. So this is, like, 4,670 pages long, right?
A. Yes, it is.
Q. Why is this on here?
A. Because this includes all of -- a directory listing of all of the files on the computer. So a majority of the spreadsheets that we just introduced or that we talked about are derivative from the file listing.
Q. Let's open the first folder. Again, this is for the user Anzor?
12:59
THE COURT: Mr. Chakravarty, if you're going to start a new topic, I think we're close enough to 1:00. We'll take a lunch recess at this point.
THE CLERK: All rise for the Court and the jury. The Court will take the lunch recess.
(Luncheon recess taken at 1:00 p.m.)
(The Court and jury entered the courtroom at 2:08 p.m.)
THE COURT: Go ahead.
Q. Good afternoon, Agent Swindon. When we left, we were just
02:09
getting to dive -- getting ready to dive into the folders of the files that are on this -- this first CD, the 1142.
Now, did you personally verify each of the files on these CDs that they came from, the computers -- for each of the computers that you were talking about?
A. Yes. The CDs were provided to me by the team. We then

went in and verified each file existed on the computer.
Q. Did you personally verify that each of these spreadsheets that describe some of the data about what was on the computer, that that data itself was, in fact, on the computer?
A. We verified -- based on the data sets that were available, yes, we verified that the data was there on the spreadsheets from the computer.
Q. You were personally verifying that, right?
A. Yes, I did.
02:10 Q. So in the 1142-10, the registry SAM file, we had talked about the user with the full name Jahar, is that right?
A. Yes, sir.
Q. And that person created an account name called Anzor; is that fair to say?
A. Yes, sir.
Q. And can a user of a Windows Operating System designate any word as their account name?
A. The user name can be -- it's a user-defined field that they could name it anything that they would like.
02:11 Q. So you can name it after your kids?
A. Yes.
Q. You can name it after your parents?
A. Yes.
Q. And so one of the account names was Anzor on this computer?

A. Yes.
Q. On the defendant's computer.
So let's go to the Anzor folder.
MR. CHAKRAVARTY: Mr. Bruemmer, if you could.
Q. Now, what is this?
A. These are four folders that look similar to the folders that were on the -- in the user folder on the 1R6.
Q. And so these are basically Windows folders? Any Windows Operating System has folders like this; most of them do?
02:11 A. Yes. They are similar to folders that would be in a user directory structure of Windows.
Q. Did the disks that includes 1142 that you brought with you today -- do they, as much as reasonable, try to marry that same structure?
A. Again, the volume of data was such that we needed to make it easily understandable and -- for today or for court purposes or trial purposes. So we tried to keep it to the best structure we could to make it look like it was in the computer where it came from or the folder that it came from.
02:12 Q. So if I click on the desktop folder, does that mean that any contents of that were on the desktop of the defendant's computer?
A. Could you click on it, please?
Q. Sure.
A. Yes. Those folders were on the desktop of the laptop.

Q. So on this laptop, on the desktop of the computer, these five folders existed?
A. Yes. So if you're sitting at your computer with your screen up in Windows, these would be folders that would be displayed or on your desktop.
Q. And there's a PDF as well on this, 1142-15, *Effects of Intention*. Was that also on the desktop?
A. Yes, it was.
Q. And you know this because you personally checked the image of the computer?
A. Yes.
Q. And that tells you the file path; it tells you where on the computer these files were?
A. Yes. We used AD Labs as the processing software, as we spoke about this morning, to go in and see the path of where the files were.
Q. Clicking on *Effects of Intention*, is this the contents of that file *Effects of Intention*?
A. It looks similar to the file that was verified, yes, or it is the file that was verified.
Q. Click on the first folder, al Makdissi. Are these three files -- were these three files within that folder?
A. Yes, they were.
Q. It's 1142-16 through 18.
Now, there was a documents folder. Is like the My

Documents folder of a Windows Operating System?
A. Windows would call it "documents," yes.
Q. And in this folder, was there a subfolder called "web cam media"?
A. Yes.
Q. And in that, was there another folder called "capture"?
A. Yes.
Q. And then there are these images?
A. Yes, those images.
02:14 Q. Were these the images that were also referenced in that spreadsheet that you earlier spoke about?
A. Yes.
Q. Then there was a folder called "downloads," is that right?
A. Yes.
Q. And were all of these -- this folder and these files in the downloads folder?
A. Yes. Those files were in the downloads folder.
Q. So clicking on an image, this was one of the images in the downloads folder?
02:14 A. It was. The only difference on this -- on the next three or this one here was that the file extension was changed to have it display as a picture.
Q. The .jpeg file extension?
A. Yes.
MR. CHAKRAVARTY: This was 1142-98 for the record.

Q. Then there were two other photos in that folder?
A. Yes.
Q. In the music folder, was there a subfolder called "nasheed"?
A. Yes.
Q. Have you heard that term before?
A. I'm familiar with nasheed.
Q. What is a nasheed in your understanding?
A. My understanding of nasheed is --
02:15 MR. FICK: Objection, foundation.
THE COURT: Overruled.
A. My understanding is that a nasheed is a sort of chant and typically popular in Islamic culture. A lot of them are in Arabic. I don't speak Arabic, so I'm not sure I would be able to recognize what they're saying, but I am familiar that they do exist.
Q. Clicking on that folder, the nasheed folder, are there a number of files number 1142-100 through 136 on that folder?
A. Yes.
02:15 Q. And these are all audio files?
A. Those are -- if you could expand it? The title, please? Yes, those are MP3 files, or audio files, yes.
Q. And there's one that's on this disk in the parent folder "music"?
A. Yes.

Q. Now, is this all of the music that was on this computer hard drive?
A. No.
Q. Then there was another folder that was specifically called "music," is that right?
A. Yes.
Q. And there was a folder called "playlists"?
A. Yes.
Q. What's a playlist?
02:16 A. A playlist is a file that is sort of like a table of contents that a Windows Media Player or a similar program would create to keep a sort of file list of songs or, say, a table of contents of songs that you would create.
Q. So I clicked on the playlists subfolder. And are there two playlists here?
A. Yes.
Q. And the WPL extension means it's a playlist?
A. It's a Windows Playlist.
Q. Windows Playlist, excuse me. Can you view that using a
02:17 text editor?
A. Yes. You could use that text editor or Notepad.
Q. Does this list in the computer code the various files that were on the playlist?
A. Yes.
Q. Now, there was another user folder called "public" on this

computer, is that right?
A. Yes. That's a Windows-created folder typically used for -- when you have sharing set up amongst computers, that the public folder would be the file or the folder where you would be able to share documents with other users.
Q. So this is the user profile that anybody who's using the computer can see?
A. Yes.
Q. And were there several files in this folder that were not exported onto the CDs?
A. These two files here were in the public folder.
Q. And opening 1142-147, is that a Microsoft Word file?
A. The extension of .docx, yes, that's a Microsoft Word file.
Q. Is this the contents of that Microsoft Word file?
A. Yes.
Q. Is the -- at the top left-hand corner of this file, is it written, "Jahar Tsarnaev, Modern World History, Miss Auty"?
A. Yes.
Q. And then the title of the document is called, *The Predator War*?
A. Yes.
Q. Opening 1142-148, is this a 578-page PDF file that's in Cyrillic?
A. It is a PDF file. In the top left-hand corner, it is recognized it is 578 pages. And I don't -- can't speak the

language, but I do recognize that as Cyrillic language.
Q. For foreign-language documents that you encountered when you were -- you and the rest of the investigative team were analyzing the various devices, what happened with those in the FBI?
A. What would happen is, if the team encountered something that they needed translated, we have a full staff of linguists who are proficient in numerous different languages that would be able to translate that.
02:20 Q. With regards to the content on these CDs, for some of the foreign-language documents, are, in fact, there translations that linguists at the FBI did and put on there?
A. Yes.
Q. Now, the files folder, I'm clicking on an exhibit marked 1142-150, "work resume." Was this in the files folder?
A. Yes, it was. No. Files folder is what we created, so this came off of the hard drive.
Q. So you called this folder "files"?
A. Yes.
02:20 Q. For files that were not in one of those other folders?
A. Yes.
Q. And so is this the resume of a person named Jahar Tsarnaev from 410 Norfolk Street, No. 3?
A. Yes.
Q. Does he list his email address as j.tsarnaev@yahoo.com and

his phone number as 857-247-5112?
A. Yes.
Q. Is it a one-page of content?
A. It appears to be two pages, but one page has the content.
Q. He lists himself as a student at University of Massachusetts at Dartmouth, is that correct?
A. Yes.
Q. The other image in this folder is called 1142-149-carved, and then there's a number. What does that mean?
02:21 A. So the forensic software that we use to process digital evidence, as we mentioned earlier this morning, has the ability to carve files out of space that is no longer being used by the computer. It's a fairly simple process. Each file has a specific header associated with it so the computer will be able to identify what kind of file that is. There's a specific header associated with a JPEG or a document or a spreadsheet. So the program will go out into unallocated or free space on the computer that's no longer being used, and it will look in that area of the computer to try and identify any of the files
02:22 that can potentially be recovered out of a space.

Once it identifies a file that it recognizes, it then continues to try and rebuild what may have been in that space before. And this would be an example of something that was carved out of free space on the computer that is now depicted as a JPEG.

Q. Go back to the Anzor account name, and I open the folder called "YE." The first document in that folder, 1142-71, has a number of blank underlines. What does that mean?
A. Sometimes the forensic software has a hard time with non-English alphabet characters. So if it was Cyrillic characters, sometimes through the processing with the forensic application, it doesn't know how to translate it. If it doesn't know how to translate it into an English equal or does not have the ability to depict the Cyrillic language, it will
02:23 replace it with typically an underscore, which is what you're seeing here.
Q. And so that particular document, is that a foreign-language document?
A. It appears to be, yes.
Q. Again, like the other documents that were in foreign language, were those given to the translators to translate?
A. I'm not sure if this particular document was, but, yes, they were given to the translators to translate.
Q. On this one, there's no translation on the CD of that
02:24 document, is that correct?
A. Correct.
Q. I'm going to go down to the file 1142-91, completeinspire.pdf. Have you seen that name throughout your analysis of these CDs?
A. Yeah. The name of that file was apparent on numerous of

the different CDs that we had or that we looked at or the different pieces of media that we looked at.

Q. In fact, on the spreadsheets that we looked at before the lunch break, did we see that in both the external drive access as well as amongst the link files?

MR. FICK: Objection. I didn't understand the question.

THE COURT: I didn't hear you.

MR. FICK: I'm not sure I understood the question.

02:24 THE COURT: Try it again.

MR. CHAKRAVARTY: I'll try again.

Q. Did the name of that file, *Complete Inspire* -- did that name appear in both the external access spreadsheets that we went through earlier as well as the file access or link history spreadsheet?

A. Yes, it was on that spreadsheet.

Q. Is this the first page of 1142-91, completeinspire.pdf? Is this the first page?

A. Yes, it is.

02:25 Q. Do you recognize it?

A. Only from seeing it -- from viewing it on the disks and the different pieces of media.

Q. So do you know what it is?

A. I know it's from -- other than reading the first page, I know it's a magazine and in -- from what it says on the cover.

Q. Does the cover call it "The Periodical Magazine Issued By the Al-Qaeda Organization in the Arabian Peninsula"?
A. Yes, it does.
Q. Is this a 67-page document?
A. Yes, it is, 67 pages.
Q. Is one of the articles, *Make A Bomb In The Kitchen Of Your Mom*?
A. That's what it says on the cover, yes.
Q. Now, you're not an expert on this document, right?
02:26 A. No, sir.
Q. Is this, on Page 33, the beginning -- apparently the beginning of the article, *Make A Bomb In The Kitchen Of Your Mom*?
A. Yes, Page 33, yes.
Q. And go through how many pages the article is. Is that a seven-page article?
A. It started on 33 and ended on 40. Yes.
Q. Going to the subfolder, the *Hereafter Series,* on the desktop under Anzor, what are these files?
02:27 A. They are -- can you display them differently, please? File details. Those are depicted by the icon on the left. They apparently -- they appear to be RealPlayer files.
Q. So the icon on the left, you mean these icons?
A. Yes.
Q. It tells you generally what kind of a file Windows

recognizes it to be?
A. Windows would associate -- with that file type would associate the RealPlayer icon.
Q. And do 1142-49 through 1142-70 appear to be different files with the name -- different titles, all of which have the name Imam Anwar al-Awlaki?
A. If you could please scroll down? Yes. They all appear to say al-Awlaki.
Q. Going now to the folder "papka," you don't know what
02:28 "papka" means in Russian, do you?
A. I do not.
Q. So there are a number of PDF files in this folder, is that right?
A. Yes.
Q. And clicking on 1142-36 called *Join the Caravan* --
MR. CHAKRAVARTY: Can we try to get that again, Mr. Bruemmer? Sorry. There we go.
Q. Is this the substance of the document called *Join the Caravan*?
02:29 A. It is labeled *"Join the"* -- it's labeled *"Join the Caravan*," yes.
Q. Is this a 35-page PDF?
A. It's a 35-page PDF, yes.
MR. CHAKRAVARTY: Mr. Bruemmer, if you can just get me back to that title screen?

MR. FICK: What's showing now is not in evidence.

MR. CHAKRAVARTY: It's not evidence. Clear the screen as well. Thank you.

The one with all the folders.

THE COURT: I've taken it down until you get to the place you want.

MR. CHAKRAVARTY: Thank you, your Honor.

I'm there, your Honor. Thank you.

Q. Back in that papka folder, is there a document in here called "Issue 9," 1142-35?

02:30

A. Sorry. Yes.

Q. Does that appear to be another issue of the *Inspire Magazine*?

A. Yes, it does.

Q. Is there a folder called "Islam" in this subfolder?

A. Yes, there is.

Q. Exhibit 1142-45 entitled, "Saif al Bader," is this a 56-page PDF?

A. Yes, it is.

02:31

Q. Does the cover page indicate that the name of the document is "The Slicing Sword"?

A. Yes, it does.

Q. Now, were these documents that were -- that you verified on these disks, were these English-language documents with the exception of the two, I think, that -- or the one, I guess --

two that we talked about?
A. I'm sorry?
Q. Were these English-language documents?
A. Not all of them were English-language documents.
Q. If they were in a foreign language, with the exception of the two that we saw, would there be a translation as well?
A. If there was a requested translation done and it was included on the disk, it would be depicted in the same path as where the file was you're seeing here.
02:32 Q. And all these are English-language titles, correct?
A. Yes.
Q. There's also 1142-41 entitled, Sheikh Anwar al-Awlaki -- sorry, "Sheikh Anwar Awlaki: The Battle of Uhud, Part 5-5, YouTube," what kind of a file is that?
A. Can you please extend the file to the right? It's an MP3 file.
Q. An MP3 file is an audio file?
A. Yes.
Q. Now, we've looked at files of a general type. Were there
02:32 other types of files on this computer?
A. Yes. There were a lot of files on the computer.
Q. What kinds of files were on the computer?
A. There was the -- just like any other computer, there was the Windows Operating System . There was a lot of other files that existed there that would be a part of a normal Windows

installation.
Q. What other types of files were there?
A. I'm sorry?
Q. What other types of files were there?
A. There were other -- when we went back into the thing to verify that these documents -- and we looked at the drive -- there was over -- as we had showed earlier in the directory list, there's over a half million files on the drive itself. So this was a representative sample that was given to us to
02:33 verify.
Q. Were there internet search histories or other things related to sports or homework or other types of topics?
A. Yes.
Q. We didn't ask you to pull those and put those on the CDs, right?
A. You did not.
Q. Let's move onto Exhibit 1143. Would it be helpful to have 1557 up for you?
MR. FICK: Just to clarify, this next one is not yet
02:33 in evidence, as I understand it, is that correct?
MR. CHAKRAVARTY: It is not.
Can we have 1557, please? Thanks.
Q. Now, what does disk 1143 correspond to?
A. 1143 corresponds to 2R14, which is the second one on the list.

Q. Is that a desktop computer that was seized from 410 Norfolk Street in Cambridge?
A. According to the list, yes.
Q. Was that also imaged and processed like the defendant's computer?
A. I'm sorry?
Q. Was that also imaged and processed like the defendant's computer?
A. It was imaged at Black Falcon and processed at Center Plaza.
Q. It was pursuant to the same protocols you had described earlier?
A. Yes.
Q. The disk that you have in front of you as 1143, did you verify that all of the information, with the exceptions of the titles of some of the documents, the exhibit numbers and the translations, that all of that content was on that computer?
A. Existed on the computer, yes.
MR. CHAKRAVARTY: I would move in 1143.
MR. FICK: Same foundational objection especially with regard to the spreadsheets.
THE COURT: Overruled. I'll admit it.
MR. FICK: And, actually, the translations. Those, I think, we got yesterday. I haven't had a chance to verify them yet.

THE COURT: Well, I'll admit it.

(Exhibit No. 1143 received into evidence.)

MR. CHAKRAVARTY: Sorry. I'm just waiting. Thank you, your Honor.

Q. Is this the file directory or the files that are in the 2R14 HP desktop folder?

A. These are the files. These are the files that are on 1143.

Q. We'll just go through them again. You can explain what they are.

What's the first folder?

A. First folder was a folder called "Umar," which, like on 1R6, was the user folder that was on the Windows machine.

Q. So somebody named this computer account Umar?

A. Yes.

Q. 1143-01, what is this?

A. This is a report that was generated utilizing Internet Evidence Finder, which depicts social media and internet activity on the desktop.

Q. Okay. Is this, like the one for the defendant's computer, it's a portion of the internet evidence that was found, correct?

A. Yes, yes.

Q. 1142-3, what is this?

A. Again, like 2R6, this is a directory listing or a listing

of the link files, or the shortcut files, that existed on -- I'm sorry. These are the files from the desktop on 2R14.

Q. And 1143-4, what is that?

A. It's the log file for the original imaging.

Q. And this lists again the person who imaged it as well as the type of hard drive it was?

A. Yes.

Q. And was this a one-terabyte hard drive?

A. Yes. That's the software that the hardware is reporting, yes.

Q. 1143-05, what is this?

A. It's a -- it's a select -- as the title notes, it's a selected user files from the computer on the Umar folders.

Q. What does that mean?

A. These folders would have existed -- or these files -- these paths would have existed in the Umar user on the computer of 2R14.

Q. Again, is this all of the activity on that computer?

A. It is not all the activity on the computer.

Q. 1143-05-A, what is this?

A. That's the complete file listing for the computer.

Q. So this is a 2,544-page document. Is this similar to the defendant's computer, or is this a listing of all the files on the computer?

A. This is a complete file listing for the entire computer.

Q. 1143-06, what's that?
A. This is the -- a list of the installed software that was on 2R14.
Q. Is this -- like you did for the defendant's computer, this is --
MR. FICK: Objection to the continued use of defendant's computer, which I don't think has been established.
THE COURT: Refer to it by its number.
MR. CHAKRAVARTY: I will, your Honor.
02:39 Q. Like you did for 1142, is this a list of the applications that were installed on this computer?
A. On 2R14, yes.
Q. 1143-07, what is this?
A. This is the file for the information that holds the security account manager for Windows, which would include the names of the users that were on that computer.
Q. So unlike the other computer that had the full name Jahar, in this case, the 2R14, there was no full name listed, correct?
A. There was no full name listed, no.
02:40 Q. Whoever set this computer up, just called the account Umar without putting their own name in?
A. Yes.
Q. Does it list on here -- excuse me -- when the last login date was?
A. The last login for the user?

Q. For the Umar account, yes.
A. Yes.
Q. When was that?
A. March 21, 20:34:07, on 2013. But, again, the Z would denote that it was Zulu time.
Q. 1143-08, what is this?
A. This is the information, like 1R6, which is the Windows installation -- or the Windows information for the computer, verifies that the licenses are -- gives the user license for the Windows and what version it's running.
Q. And 1143-09, what is that?
A. This is an internet activity history report.
Q. Is this also generated with the Internet Evidence Finder tool?
A. Yes.
Q. Again, is this a partial internet history?
A. The data that's on this spreadsheet was generated from Internet Evidence Finder.
MR. FICK: Again, object to the translations as I'm seeing them for the first time now.
THE COURT: All right.
Q. This is a 20-page document, is that right?
A. Yes, it's a 20-page document.
Q. And like the spreadsheet that we saw on the previous computer, there are dates on some of the entries, and there are

no dates on some of the entries?
A. Yes.
Q. So let's pick a couple of these to focus in on. So this file here, it says, "J:completeinspire.pdf." What does that entry mean to you?
A. On the column on the right, all the way -- I'm sorry, all the way to your right. The Internet Evidence Finder would have grabbed this information out of what we would call -- okay -- the "U" would be for unallocated space. So that remnant or
02:43 that file structure, that file name, was recovered by Internet Evidence Finder and shows possibly at some point that file -- that this file was accessed on this computer by -- on a J drive.
Q. What's the J drive?
A. The J drive -- J would be the file letter that Windows would give whatever -- the next one in line or assigned by a user to a removable media device or something that was plugged into the computer.
Q. There's a date over here. What does that date correspond
02:44 to?
A. Well, because it came out of an unallocated space, the date really -- it's not really very reliable.
Q. Okay. And you say "unallocated space." Do you know that because of --
A. Because of the --

Q. This U?
A. Yes.
Q. What does unallocated space mean?
A. That's the portion of the computer that we talked about earlier where it's sort of the space that's not being used by the hard drive or by the operating system or by any applications anymore.
Q. Now, going down a few entries, we see the same file name being accessed on the J drive, right?
02:44 A. Yup, yes.
Q. And that's an allocated space, right?
A. Yes.
Q. And what's the date of that access?
A. 12/26/2012, at 2:39 p.m.
Q. Now, this email address, j.tsarnaev@yahoomail, is that the email address that was on the 1R6, the Exhibit 1142 user profile?
A. That was in the -- that was in several locations on 1R6.
Q. Excuse me. That wasn't on the user profile. I think it
02:45 was on the resume?
A. Yes.
Q. Does it show that that access, according to the Internet Evidence Finder, that email account was accessed on New Year's Day?
A. Right.

Q. On 2013?
A. Right. If we look at the column to the left, that's going to give you the URL or the web page that was accessed, that it grabbed as a part of the history. And that's the -- the Internet Evidence Finder generates that middle column, and it then associates the date and time with that activity -- internet activity.
Q. This column called "title," this column, what kind of data is indicated in that?
02:46 A. Well, the title is generated by the Internet Evidence Finder. It types -- it's the type of traffic that it recognizes.
Q. And the various content of these columns, what does that indicate?
A. Did you want me to read every single one?
Q. No. Just for the first one, what does it say, if you can read it?
A. It says, Junies Uderoff (ph) Google search.
Q. What does that tell you?
02:46 A. It says that that string to the left would be something -- if you were going to go to Google.com and do a search for something, and you typed, for example, that name in the box in the middle of Google and sent that search request back to Google, that's -- the string on the left would be the actual request going back to Google. So Internet Finder would parse

out that information, recognize that it's a Google search, and include that in the title.

Q. So I just underlined the entry in the URL field. Is that what you were talking about?

A. Yeah. Actually, you can see -- if you go up to the first line, you can see -- after Google.com, you can see the search term there.

Q. And so on the entry that says, "Anwar Awlaki Abu Bakr (RA), Part 1/8, YouTube," does that mean that that website titled that was accessed on January 1, 2013, at about 3 p.m.?

A. If you look to the left, again, Internet Evidence Finder identified the URL on the computer as being that number or that URL and then associated it with that file name -- or with that name and then created the date visited.

Q. I'm going to go through a few more pages and then move on. Are these -- in the URL column, are these various websites that were visited?

A. In the URL column, Internet Evidence Finder would have parsed out through the internet history files associated with all the different browsers that are available and then would have been exported to this report. So, yes, these are -- those are websites that would have been visited.

Q. So those websites like ghuraba.info, Jamaat Shariat, as well as Netflix?

A. Yes.

Q. There's a lot of entries for this website called Kav Kaz Center. Did you see that throughout this computer?
A. I recognize that from the report, yes.
Q. And the -- for a lot of the Kav Kaz entries, there is Cyrillic writing; is that fair to say?
A. That's -- I recognize it as Cyrillic writing, yes.
Q. Now, just as we had talked about the general content that was on the 1R6, the Sony Vaio laptop that's numbered 1142, was there a variety of different types of content on the 1143 desktop that was seized from Norfolk Street?
A. There was a variety of different files on the computer, yes.
Q. And were you able to determine whether this was used by only one person or many people?
A. Given -- as we spoke this morning about combining the investigative information with the information that's on the computer, I think it was used by many people.
Q. 1144, what does that correspond to?
A. Back to the report, 1144 corresponds to 3R4, which would have been a thumb drive designated as Micro Center, two-gigabyte thumb drive, seized from the Pine Dale Hall and imaged at Black Falcon and processed at Center Plaza.
Q. Pine Dale Hall you know is a dormitory at the UMass Dartmouth campus?
A. Yes.

Q. And "TD" means thumb drive?
A. Yeah. That was our designation, yup.
Q. As with the computer devices, did you confirm that the contents on the disk 1144 reflects a selected portion of the contents of that thumb drive?
A. Yes.
MR. CHAKRAVARTY: I'd move in 1144, your Honor.
MR. FICK: Same objection.
THE COURT: Same ruling. Admitted.
02:51 (Exhibit No. 1144 received into evidence.)
Q. So in the 3R4 folder, what do we see here?
A. 3R4 folder, there are a file listing PDF, a text file, which is a log file, as we've looked at the other two. And there are two files that were found on that thumb drive.
Q. And so the first folder says "carved files." What does that mean?
A. As discussed earlier, when the software application that we use has the ability to carve files out of that unallocated space where a file may have previously been. Those would have
02:52 been files that were associated with that process of carving that were identified by the software application.
Q. Let's click on 1144-01. What is this?
A. It's a file listing for the 3R4.
Q. So unlike the computers, which have thousands of pages of files, this only has three. Why is that?

A. It's a smaller device. It doesn't have an operating system. And it would be used just to transfer files.
Q. 1144-02, what is this?
A. It's the log file. The log file for FTK Imager, which was used to image the thumb drive.
Q. Again, this also shows how much storage you had on this --
A. Yes.
Q. -- on this -- I'm just trying to find out how much storage that is. Can you tell?
02:53 A. It's approximately two gig.
Q. Two gigs, all right.
1144-05, completeinspire.pdf, is that the same file or same document that was on the -- both of the two computers we've seen already?
A. With the visual inspection, yes.
Q. In fact, I actually hadn't done that with the second computer so go back a second.
I went through the spreadsheets with you on the desktop computer, but I didn't go through each of the user
02:54 files. I'll try to do it quickly.
MR. FICK: Could we make sure the record is clear what exhibit we're in?
MR. CHAKRAVARTY: Sure. We're back on 1143.
Q. On the desktop, were there a number of folders in the desktop?

A. Yes.
Q. There were subfolders as well?
A. Yes.
Q. And they had audio files just like the other computer?
A. Yes.
Q. And they had these YouTube files as well?
A. Yes.
Q. They had a folder called the *Hereafter Series* also?
A. Yes.
02:54 Q. And like the 1142, it had a number of Anwar al-Awlaki documents or audio files in that folder?
A. Yes. Could you change the view to details, please?
Q. Sure.
A. Yes.
Q. And in 1143, it was 1143-43 to 1143-64 that were all these Anwar al-Awlaki audio files, correct?
A. Yes.
Q. Then there were a number of documents on the desktop that would be visible to somebody who was accessing that user
02:55 account, correct?
A. Yes.
Q. The documents folder went into subfolder called "blio," subfolder entitled "tema." Is there a document called 1143-69, *Inspire*, March 2011?
A. Yes.

Q. And that reflects another copy of *Inspire Magazine* for a different issue?
A. Yes.
Q. Now, that March 2011 magazine has this picture and the title called, "The Tsunami of Change," is that correct?
A. That's what's depicted, yes.
Q. Going back now to where we had left off at 1144, which was the thumb drive that was found in the defendant's dorm room, is that right? Sorry. Do you need the chart again?
02:56 A. 1144 was -- yeah, Pine Dale Hall, yes.
Q. Now, in the carved files, what are these?
A. Again, the forensic software is able to carve files out of that -- the unused space on that device by that process of identifying a file header and trying to capture as many or as much of that files as it can. And it carved JPEGS out of the unallocated space on the thumb drive.
Q. I called up 1144-07-24. Is that the same JPEG or image file of the cover of the Spring 2011 issue of *Inspire Magazine*?
A. That's a JPEG, a single JPEG, depicting the first page of
02:57 the PDF that we looked at.
Q. So it's not -- what you were able to recover on the thumb drive was not the entire PDF document but rather a series of images or JPEGS, correct?
A. Yes.
Q. Did you verify that that's, in fact, what all of these

images are?
A. I'm sorry?
Q. What are all of these images in this folder?
A. These are carved images out of the unallocated space on the thumb drive that match photos or images that are on that -- the March 2011 *Inspire Magazine*.
Q. In addition to that *Inspire* -- issue of *Inspire Magazine*, was that *Complete Inspire* magazine that we had seen before also on there?
02:58 A. In PDF form, yes.
Q. Was this in the active space so it wasn't carved? It didn't have to be recovered?
A. I'm sorry. Yes, it was in active space.
Q. In addition, 1144-06, was this a scanned document that was on the thumb drive?
A. Yes.
Q. What does it appear to be?
A. It appears to be a pay stub for Katherine -- from Donald Larking, 1600 Washington Street.
02:59 Q. It was found in the defendant's dorm room?
A. The thumb drive was found in the dorm room, yes.
Q. Let's move onto 1145. What is that?
A. 1145 was the files extracted from an iPod Shuffle.
Q. And 1146?
A. 1146 was from an iPod Nano.

Q. And the files on those CDs, are those, like the other ones, you verified that they're actually on those items of evidence?
A. Yes.
Q. Were those iPod -- the iPod Shuffle and Nano found in the Honda Civic that was recovered in Laurel Street?
A. If you could bring back up --
Q. Sure, sorry.
A. Yes.
03:00 Q. Those are the items that actually already have been introduced in this case?
A. Yes.
MR. CHAKRAVARTY: I'm sorry. I would move in the data collected from 1145 and 1146.
MR. FICK: Same objection. Foundation, improper confrontation.
THE COURT: Admitted.
(Exhibit Nos. 1145 and 1146 received into evidence.)
Q. I've opened 1145. Can you explain this structure?
03:00 A. 1145 would have been the -- an iPod Shuffle. So the text file would show the imaging log for the imaging of the device.
Q. And I'm first opening 1145-02. What is that?
A. That's the log file for the imaging that took place on that.
Q. 1145-01?

A. Is a derivative file list, a file list of files that were found on the iPod Shuffle.
Q. So this is some of the audio files that was on the iPod Shuffle?
A. Yes.
Q. And 1145-01-A?
A. Is the complete file list of all the files that were found on the Shuffle.
Q. So the previous exhibit was a subset of this?
03:01 A. Yes.
Q. Under "files," are these that subset of the audio files that were on the computer -- excuse me, on the iPod?
A. I'm sorry?
Q. Were these a subset of files that were on the iPod?
A. These files we verified were on the iPod, yes.
Q. 1145-24, entitled, "The Man Who Went to Jannah Without Praying, MP3," did you see that in your verification of other devices?
A. I recognize the title from other places.
03:02 Q. Do you remember which other devices that was on?
A. I don't. But if I had the directory listings, I'd --
MR. CHAKRAVARTY: Can we call up just for the witness 1553, please. Court's indulgence, your Honor.
I'll move on in the interest of time and come back.
Q. Let's go to 1146, which is the other iPod that I believe

I've moved into evidence now. On this iPod, the 1146, there are four-digit names for files. Why is that?
A. I'm aware that the iPod, or the iTunes software, when they install the MP3s or the files on of the device that it changes the name of the file and creates a pointer to that. So if you go back, there will be, like, a playlist, as you had recognized from all of your songs, and it creates that -- the playlist would create pointers to those files.
Q. And 1146-01, is this a derivative file listing, listing those files?
A. Yes, it is.
Q. 1146-01-A, is this the complete file listing for all the files on that --
A. Complete file listing of everything that was on the device.
Q. And 1146-27, is this a log file?
A. Yes.
Q. It's listed as an iPod, Apple iPod device?
A. Yes.
Q. Now, were you -- did you compare whether some of the audio files were common across various devices?
A. Yes.
Q. Okay. Explain what you did.
A. Well, we -- I mean, when we recognized the names across several of the devices, we -- when we were going through

verifying and validating, we recognized that some of the titles were the same and played them to verify that they were on the devices.

Q. So some of the iPod files that come in four-digit titles, did you verify that those files were actually also the same files that were -- the same audio files that were on some of these other devices?

A. It's difficult to do through just listening, but we did use another process to verify that they were the same.

03:06 Q. What was that process?

A. We talked earlier about the MD5 hash values. We use them to verify images of computers, but we can also use them to compare files. So if we created an MD5 hash value for a file, we then could run that -- find that value in other places, and then it would show scientifically that it was the same file.

MR. CHAKRAVARTY: Now, your Honor, just for the witness, please, 1438, please.

Q. Do you recognize what this is?

A. It's a spreadsheet that was put together by the team that

03:07 was depicting the propagation of the files.

Q. All right. Did, actually, you create an updated version of this particular spreadsheet?

A. There's an updated version of this spreadsheet, yes.

Q. Does that updated version actually compare the MD5 hash values?

A. It does. It includes the MD5. We added a column of the MD5 hash values for each of the files across the devices.
Q. What commonalities did you find over -- after looking at the MD5 hash values?
A. If the hash values matched, the file is essentially the same or is the same. So we just compared the MD5 hash values. And once we were able to show that it was the same across all of the devices, we can verify that it's the same files.
Q. Did you, in fact, find that some of the audio files were
03:08 the same across various devices?
A. Yes.
Q. What were devices that you found being similar across the --
A. 1R6, 1437, 14-6, and 3R5.
Q. We haven't discussed 3R5 yet, right?
A. We have not.
Q. Were these particular audio files that were common across those devices?
A. They were MP3 files.
03:08 Q. Particularly the file that I had just clicked on but haven't played is, "The Man Who Went to Jannah Without Praying." Was that one of them?
A. Yes. That was one of them that was common all across all four devices.
Q. Was there also another audio file called "The Most Amazing

Nasheed" that was common across all four devices?
A. Yes, across all four devices, yes.
Q. Was there also the file called "The Most Wonderful Nasheed" that was common across all four devices, although the title of the file was different?
A. Yes.
Q. So was that -- did the MD5 hashes compare favorably on that? How does an MD5 hash stay the same if the file name changes?
03:09 A. It doesn't change any substance of the file. This could have been a pointer. If you could -- I'm sorry. So depending on how the file was handled within the device or the iPod, it wouldn't make any substantive changes to the file which wouldn't change the MD5.
MR. CHAKRAVARTY: All right. Thank you, Mr. Bruemmer. Go back to the other screen.
Q. The 3R5, does that correspond with Exhibit 1141?
A. Yes, it does.
Q. I've just called up 1557 again. What was the 3R5?
03:10 A. The 3R5 was a Samsung Finesse cell phone seized at the Pine Dale Hall location. It was imaged at Black Falcon and processed at Black Falcon.
Q. Again, was this a cell phone found in the defendant's dorm room?
A. Yes.

Q. And was this one of the devices that had those audio files on it?
A. Yes, it was.
MR. CHAKRAVARTY: I'd move in 1141 into evidence, your Honor.
MR. FICK: Same objection.
THE COURT: All right. Noted and admitted.
(Exhibit No. 1141 received into evidence.)
Q. Now, this is the first cell phone that we're looking at the digital extraction for, is that right?
A. Yes.
Q. So what do we see here in the UFED Samsung CDMA SCHR810 finds?
A. Cell phones are processed a little differently. They're several different ways we can process cell phones. One way is through a product called UFED, or CelleBrite. And that's how this phone was imaged. And it creates a report from the phone and allows you to extract the files from the phone.
Q. The first file, 1141-01-07211546.jpeg, what's that?
A. It's a JPEG that was extracted from the phone.
Q. Were there several other JPEGS or image files that were found on this phone?
A. Yes, there was.
Q. You didn't extract them all, right?
A. I was asked to verify this was on the phone.

Q. Were there other pictures of the defendant on that phone?
A. Yes, there were.
Q. What is this?
A. This is a copy of the phone examination report.
Q. Is this something that the software generates?
A. Yes. This is software-generated.
Q. What type of information is in this 131-page document?
A. This would -- depending on the type of phone and the process used, this could include contacts, text messaging, photos, files that were on the phone. It would include maybe the SIM card information if there was a SIM card associated with the phone. It would be anything -- or data that would be associated with the phone.
Q. Does it also include the phone contacts?
A. Contact lists, yes.
Q. So I'm just going to scroll through the list of contacts here. Is that about 17 pages of contacts?
A. Which page did you start on?
Q. Sorry. I start on Page 2.
A. 2 to --
Q. 2 to 18?
A. I can't really tell because the pagination might not be right, but it's on or about --
Q. Thank you.
A. -- that number pages.

Q. Then there's some call data here?
A. Yes.
Q. And is the call data obtained from the phone handset or from the telephone company that provides service?
A. This report is generated from data that's on the phone.
Q. In your experience as a computer forensic examiner, have you compared whether phone data from a handset is the same as phone data from a cell phone company?
A. I mean, it would be a separate legal process, but you would have to subpoena the phone records or -- and do a comparison.
MR. FICK: I'm actually going to object to this version of this exhibit which appears to have lost the image -- I'm sorry. I'm objecting on completeness grounds because it looks like this version that's now the exhibit has lost the image thumbnails that go in the report.
THE COURT: You can examine on it. We'll deal with it if --
Q. These are bookmarks for a variety of different images that were taken on the phone?
A. On the left-hand column is the information that is -- is the file names that were on the phone, yes.
Q. And looks like there are hundreds of images on this phone, right?
A. Yes.

Q. And then, in addition to images, are there audio files on this phone?
A. Yes.
Q. And, again, like the images, all of these -- the audio files themselves are not on this disk, correct?
A. They are not.
Q. I'm just getting to the bottom. It looks like there's over a hundred audio files in this phone as well?
A. Yes.
03:15 Q. Then there are some video files, correct?
A. Yes.
Q. And all of that data was not exported to these CDs, correct?
A. It was not.
Q. Going into the audio folder on this now, was this the folder that contains the files that were actually extracted and put on the CD for the jury?
A. Was that the actual folder that was on the phone?
Q. No. Was the folder on the CD --
03:16 A. Yes.
Q. Does that contain the actual files that --
A. Yes. These audio files were on the phone, yes.
Q. So this is not the hundreds of audio files that may have been on the CD?
A. No, no.

Q. Can we just go through and read the titles of these files that were on the Samsung phone?

MR. FICK: Objection. It speaks for itself.

THE COURT: Sustained.

Q. Is it fair to say that 1141-03 through 1141-11 were all audio files that were on the Samsung phone?

A. Yes.

Q. And several of them were also on those other devices that you just described, the two iPods as well as the laptop computer, the Sony Vaio?

A. 1R6, yes.

Q. 1R6. Let's move onto the next CD. I think it's 1147 -- 1147 and 1148. What are those?

A. 1147, 1148 correspond to 2V7B and 32-2. They were CD-ROMs. One was seized -- or identified and seized in the Honda Civic. It was imaged at Center Plaza, processed at Center Plaza, and contained audio files. And 32-2 was a CD-ROM seized in the Mercedes, imaged at Center Plaza, processed at Center Plaza, and contained audio files.

Q. And so these were the two CDs that were found in the two vehicles that were in Watertown on April 18 and April 19, 2013?

A. Yes. They were found in the Honda Civic and the Mercedes, yes.

Q. The Mercedes one, do you recall if that was the CD that was in the radio that they -- the state police was able to get

out?
A. I didn't seize it from the Mercedes but, according to the description and the location, yes.
Q. And the other CD, was that the one from the Honda Civic? I think it was in the glove box?
A. Yes.
Q. And, again, did you extract -- did you verify that the data on the extracted CDs that you have in front of you is, in fact, data from those two CDs?
03:18 A. Yes.
MR. CHAKRAVARTY: I'd move in Exhibits 1147 and 1148.
MR. FICK: Same objections.
THE COURT: All right. Admitted.
(Exhibit Nos. 1147 and 1148 received into evidence.)
Q. 32-2, the folder marked 32-2, which is in 1147, is this the one-page file listing of the files on that?
A. Yes.
Q. 1147-03, is that a playlist for the CD?
A. Yes.
03:19 Q. Clicking on the files folder, is this the file structure that was on that CD?
A. Those were the files that were on the CD, yes.
Q. And for 1147, in the parent folder under "files," are there several documents with the name Sheikh Anwar Awlaki in them?

A. Yes.
Q. At least Exhibits 1147-09 through 1147-16?
A. I'm sorry?
Q. Sorry. Do those -- just for the record, I just wanted to make clear which of those files we're referring to. 1147-09 through 1147-16, do these all start with "Sheikh Anwar Awlaki and the Battle of Badr and the Battle of Uhud"?
A. Yes.
Q. Each of the subfolders themselves have additional files? Some appear to be in a foreign language, correct?
A. Yes.
Q. If we go to 1148, do we see similar file structure?
A. Yes.
Q. Instead of those Sheikh Anwar Awlaki Battle of Uhud and Battle of Badr, we see, "Minor Signs of the Day, Anwar Awlaki, the *Hereafter Series*," 1148-07 through 1148-11, correct?
A. Yes.
Q. And then, like the other CD, there are a variety of additional folders which themselves have audio files in them, is that correct?
A. Yes.
Q. Like the other CD, did you verify that this was the file listing on the CD?
A. Yes.
Q. Now, this is -- again, is this all of the files on them or

just a select files?
A. This was all of the files.
Q. What is this, 1148-02?
A. This was a different -- these are -- as opposed to the log file, as we had previously -- these are screenshots that are depicting the same information that would be available in that log file.
Q. Does a CD have to be processed differently than a cell phone or a thumb drive or a computer?
03:22 A. I mean, the imaging process is different because you're using maybe a different device, but the forensic process is similar.
Q. And this 1148-05, what is that?
A. It's an FTK image or log file. So there's a bit of redundancy here because the same information is --
Q. Sorry. The same information is?
A. Is in the previous screenshots.
Q. In the screenshots, right.
Can we go to 1149, please?
03:23 A. 1149?
Q. Yes, please.
A. Is a thumb drive corresponding with 1W15. Media description is a Patriot thumb drive, seized or found at the Watertown, Laurel Street, location. It was imaged at Black Falcon, processed at Center Plaza.

Q. Now, Patriot thumb drive, is that the brand of the memory that allows -- that's put onto a memory stick?
A. What Patriot designates -- I believe designates the type of thumb drive it was. Like, there are different brands, and this happened to be a Patriot thumb drive.
Q. Does the Patriot also sub-brand out their memory so they can be branded in different ways?
A. That, I don't know.
Q. The contents of that thumb drive, was that -- excuse me.
03:24 Was that thumb drive found in Laurel Street in Watertown?
A. That's the search location it was seized from, yes.
Q. We had seen earlier on the -- on a couple of these histories, the spreadsheets that you had described earlier, a Patriot external device plugged into a phone. Is this the same device?
A. It is not.
Q. How do you know that?
A. Well, when a -- there's a -- a thumb drive has a unique serial number associated with it. So when you put it into a
03:24 computer, the registry would record that serial number. And it sits in the registry until either it's removed or the registry would make a change to it. But that serial number is collected in the registry.
Q. And so the contents of 1149, is that -- are the contents of that CD files from the Patriot thumb drive marked as 1W15

that was seized in Laurel Street?
A. Are you going to --
Q. Yeah.
A. Yes. The files from the thumb drive are on the CD.
Q. Not all of them, though?
A. If you could open the file up, please?
MR. CHAKRAVARTY: Well, I'd move into evidence 1149 first.
MR. FICK: Same objection and a relevance objection on this one, which I could explain perhaps at sidebar.
THE COURT: All right. I'll see you.
(SIDEBAR CONFERENCE AS FOLLOWS:
MR. FICK: So, as far as I understand, the only real content of this thumb drive is some of Dias Kadyrbayev's homework. So other than the fact it was found on Laurel Street, I'm not sure what it has to do with the case.
MR. CHAKRAVARTY: It just goes to the association. It's not the substance of the content. We expect the defense is going to say that everything on Laurel Street was Tamerlan's. This was actually the defendant's friend's stuff.
THE COURT: Okay.
. . . END OF SIDEBAR CONFERENCE.)
(Exhibit No. 1149 received into evidence.)
MR. CHAKRAVARTY: Your Honor, may I go ahead and publish 1149?

MR. FICK: Just note the objection.

THE COURT: Yes, okay.

Q. 1149, 1149-01, is this the file listing?

A. It is a derivative file listing.

Q. So this is a portion of what was on there?

A. Yes.

Q. And does it list apparently some homework and some things about Kazakhstan?

A. Yes.

03:27 Q. 1149-01-A, this is the more complete file listing?

A. Yes.

Q. Again, a log file?

A. Yes, of the imaging.

Q. Of the image. Then there's just a couple of homework assignments in here that are on that CD, correct?

A. Yes.

Q. I'm going to click on 1149-03. This appears to be some kind of a term paper or something called, "The Definition and Examples of Manifest and Latent Function in Society"?

03:28 A. Yes.

Q. Is the name at the top Dias Kadyrbayev?

A. Yes.

Q. And do you know that Dias Kadyrbayev was one of the defendant's friends?

MR. FICK: Objection.

THE COURT: Sustained to the form of the question.
Q. Do you know who he is?
A. I do know who he is.
Q. Who do you know him to be?
MR. FICK: Objection, basis of knowledge.
THE COURT: Overruled.
A. During my involvement with the initial investigation and in the command post, the name was recognized both to me as a part of the investigation that was going on in the New Bedford area.
Q. 1149-04, is that another homework assignment?
A. Yes, it is.
Q. Again, it's from the same person, Dias Kadyrbayev?
A. Yes.
Q. Now, at some point did you actually examine Dias Kadyrbayev's cell phone?
A. I did. Similar to the process here, I verified and validated that there was information on the phone.
MR. CHAKRAVARTY: And just for the witness, your Honor, 1553 -- I'm sorry. Did I say that wrong here? 1153.
Q. What do you recognize this to be?
A. As titled, I recognize it to be text messages from Dias' phone.
Q. In fact, with respect to communications between Dias and the defendant's phone number, 857-247-5112, did you verify that

these text message exchanges were actually on Dias Kadyrbayev's phone?

A. Yes.

MR. CHAKRAVARTY: Your Honor, I'd move to introduce 1153 for -- primarily for the communications between the defendant and Dias, not the extraneous communications.

MR. FICK: Well, I think I have the same objections as before, and then perhaps we ought to have a redacted exhibit if they're only offering it for --

03:30 THE COURT: I agree. I won't admit it unless it's redacted.

MR. CHAKRAVARTY: We'll do that, your Honor.

Mr. Bruemmer, we can go back to --

Q. Can we go now to Exhibit 1150? What is that?

A. 1150 is a -- corresponds with the Kingston thumb drive, 1B2734L14. Location was the Crapo landfill. It was imaged at Quantico and processed at Center Plaza.

Q. Was this a thumb drive that was found in a backpack that was found in the landfill down in New Bedford?

03:31 A. Yes.

Q. Does 1150, the disk in front of you, reflect files that were on that thumb drive?

A. Yes.

MR. CHAKRAVARTY: I'd move 1150, your Honor.

MR. FICK: Same objections.

THE COURT: All right. Admitted.

(Exhibit No. 1150 received into evidence.)

Q. Now, we'll go to 1150-01-A. Is this the complete file listing?

A. Yes.

Q. 1150-01-B, is this the X-Ways derivative file listing?

A. It's a derivative file listing. It's a derivative list or derivative file that was made from the other information on the complete list.

03:32 Q. Does this also include a translation column?

A. Yes, it does.

Q. And so, again, was that created by FBI translators to explain what the foreign language was?

A. Yes, it was.

Q. 1150-01, what's that?

A. It's an additional derivative file listing from the drive.

Q. This doesn't have that translation, correct?

A. It does not.

Q. 1150-02, what's that?

03:32 A. It's the log file showing the imaging.

Q. And 1150-03, are these translations for some of those foreign language files?

A. Yeah. That -- yeah. This was not on the thumb drive, so I did not verify that it came from the thumb drive because it didn't. But it's added to the data set because it includes

translations from the files that are on there.
Q. So that the jury can understand what those files are?
A. Yes.
Q. Let's open the folder "carved, recovered files of interest." What are these?
A. Back to the carving process again, the -- back to the carving process again, it recovers files from unallocated and deleted space. And also -- these are also -- in this file is carved and recovered, so there are carved files and also
03:33 recovered files, which are, as we spoke before, stuff that's recovered from deleted space.
Q. Now, are carved files always able to be recovered in the sense of being able to access and treated like as if they had never been deleted?
A. Carved files are kind of hit or miss. If it can recover part of the file, it will -- the application software will do as much as it can to render what it would -- what it used to be or using the data that it can get back. But it's not -- it doesn't always be able to render the entire file. So, for
03:34 example, if it was a JPEG, it may render only half of the file, and the bottom may be pixilated, and you may not get the entire file back.
Q. So the files on this, 1150, on this piece of media, were all of these files that we can see the titles of, are all of them able to be opened and accessed?

A. Can you scroll down to see the -- they should be able to, yes.
Q. Okay. Is it possible that some of them are corrupted?
A. I'm sorry?
Q. Is it possible that some of them are actually corrupted and you can't open them?
A. Yes.
Q. So they appear as if they're an intact file, but you can't actually open it?
03:35 A. Exactly, yes.
Q. So why would that happen in the carving process?
A. If it can't get the whole file back and it knows that it's a PDF, Adobe or another application might try and open that file. And when it doesn't have all of the data from that file, it doesn't allow it to open.
Q. I'm going to click on 1150-34. Did we get an error saying that it can't be opened?
A. Right. That would be an example. So it was able to recover the title of the file and maybe a portion of the data
03:35 but not be able to be opened.
Q. So I opened a file called 1150-14-169, "A Message to Every Youth." Is this a document that on the top says, "At-Tibyan Publications, A Message to Every Youth, by the martyred Imam Abdullah Azzam"?
A. Yes, it is.

Q. Is this a 28-page document?
A. Yes, it is.
Q. Which is in English but also has Arabic in it?
A. I'm not sure if that's Arabic, but, yes, it's English in there.
Q. At the end of this document, is there also a section called, "Also available from Tibyan Publications"?
A. Yes.
Q. Does this list other titles of documents?
03:36 A. Yes.
Q. Now, opening 1150-09-02, does this appear to be a scanned document that was also found on this thumb drive?
A. Yes.
Q. Again, this was also in carved space?
A. It was either recovered or carved.
Q. And it was in the folder called "carved, recovered files of interest"?
A. They're both carved and recovered files.
Q. Yup, carved or recovered. Does this appear to be a rental
03:37 application from a -- prepared by Katherine Tsarnaeva?
A. Yes.
Q. Do you know who she is?
A. The defendant's sister-in-law is what I know.
Q. Go on to 1151. What is that?
A. 1151 is one CD containing the reports for 2W1 and 2W2,

which is an iPhone 4s and an iPhone 5, from Watertown, on Franklin Street. They were both attempted to be processed. They were processed -- imaged down at Quantico, processed at Quantico. The phones were physically broken, as noted there, and the only data that could be collected from it was the SIM data, or the SIM card.

Q. Were these the two phones that were found nearby to where the defendant was arrested?

A. Yes.

03:38 MR. CHAKRAVARTY: Mr. Bruemmer, if we could just call up Exhibit 810, which is in evidence?

Q. Are these those smashed phones?

A. Without looking at the serial -- they appear to be the smashed phones, but without being able to verify the serial number, yes.

Q. Where were these sent?

A. Down to Quantico, Quantico, Virginia, the lab. I'm sorry.

MR. CHAKRAVARTY: Could we go to 811.

Q. 811, did you see these phones shortly after they were

03:39 seized?

A. Yes. They came into -- they came into the lab, but they were -- came into evidence -- the Evidence Response Team before they were shipped down to Quantico.

Q. As you did with Dias' phone and with the Samsung phone, did you attempt to extract the data that was on these phones?

A. Because -- due to the conditions of the phones, it was impossible to extract the data from the phones.
Q. So what did you do?
A. They were shipped down to Quantico, to the lab, to attempt to try and extract the information. They have different techniques that we don't have available to us in the field.
Q. Were they able to do that?
A. They were unsuccessful also.
Q. Was there any part of the phone from which they were able
03:40 to get any data from?
A. Well, the phones themselves contain SIM cards. As we had mentioned earlier, the SIM card is a small sort of almost like an SD card that would go in your phone. The SIM card has a unique serial number which is associated with that SIM card. The SIM cards are utilized by the carriers to authenticate your phone. And on that SIM card will have information such as your telephone number and -- potentially the telephone number, serial number of the phone, and, in Apple's case, not much more information than that.
03:40 Q. Was the lab able to extract information from the SIM card?
A. The SIM cards were imaged, yeah. There was an extraction done of the SIM cards, yes.
Q. Did that also happen back at Center Plaza when you were --
A. Yes, we did -- yes.
Q. So on Exhibit 11 -- excuse me, 1151, what exists on that?

A. 1151 are the reports from the SIM cards.

MR. FICK: These are not in evidence yet, as I understand it.

MR. CHAKRAVARTY: They're not. I'm going to move it in now.

MR. FICK: The screen is up.

MR. CHAKRAVARTY: I haven't gone to it yet. At this time, I'd move in 1151, which is the content of the SIM card reports.

03:41 MR. FICK: Same objections.

THE COURT: All right. Admitted.

(Exhibit No. 1151 received into evidence.)

Q. Now, Agent Swindon, was one of the phones given the alphanumeric identifier of 2W1 and the other given 2W2?

A. Yes.

Q. Going first to 2W1, are these a series of images of that item?

A. Those are images taken, yes, of that item.

Q. These are just evidence images of the bag and the remnants

03:42 of the device?

A. Yes.

Q. And then I'm opening up 1151-10. Is this a photo of the SIM card?

A. This is a SIM card mounted in sort of a tray-type piece.

Q. So unlike the other exhibits which you've talked about,

this actually has images of the item that you extracted data from?
A. Yes.
Q. Are those fair and accurate images of what the device looked like?
A. Yes.
Q. Now I'm opening up 1151-14-report. Is that an Internet Explorer file -- sorry, an HTML file?
A. Yes. That's the format that the forensic process or the
03:43 UFED CelleBrite presents the report in.
Q. So what is this that we're looking at now?
A. This is the report.
Q. And does it list the ICC ID number up here?
A. Yes, which is unique to the SIM card. And if you scroll down in the report, you'll see the phone number.
Q. Is this the phone number here?
A. Yes.
Q. 617-286-9151?
A. With this SIM card, yes.
03:43 Q. Do you know that to be the phone that was subscribed to by Jahar Tsarni on April 14, 2013?
A. I don't have that information here in front of me.
Q. Is that one of the two phones that was subscribed to Jahar Tsarni?
A. Yes.

Q. Let's go to the other one. Does this also have a number of images of the device?
A. Yes.
Q. And both in the evidence bag as well as outside the evidence bag?
A. Yes.
Q. And also has pictures of the SIM card?
A. Yes.
Q. Are all of those fair and accurate?
03:44 A. Yes.
Q. Clicking on the report, is this the SIM card extraction report for 2W2, the other phone?
A. Yes.
Q. Does this show both the unique ICC ID number --
A. For that SIM card, yes.
Q. -- as well as the phone number?
A. Yes.
Q. Is the phone number here 857-247-5112?
A. Yes.
03:44 Q. Is that the same number that was on the defendant's resume?
A. Yes.
Q. Was that the same number that was on Dias' phone?
A. In the text chat, yes.
Q. Now, were you able to extract any other information from

the phones that were destroyed?
A. They were unsuccessful in extracting any other information off of the chips or off of the phones themselves.
Q. Does that mean --
A. The only thing that was available was the SIM card.
Q. Were you able to get any of the content off the phone, like internet surfing history?
A. No.
Q. How about any songs or video files?
03:45 A. No.
Q. Any documents that had been accessed?
A. No.
Q. Any chats or communications with anyone?
A. No.
Q. Now, earlier -- it must be my head cold, but I think I asked you whether you had Exhibit 1457 in that folder. I meant to ask you if you had Exhibit 1475 in that folder.
A. Yes.
Q. What does Exhibit 1475 correspond to?
03:46 A. 1475 corresponds to a -- the 1W16 CD external hard drive, was seized in Watertown, Laurel Street. It was imaged at Center Plaza, processed at Center Plaza.
Q. Was that the hard drive that was found on the street in Watertown after the shootout?
A. Yes.

Q. Does 1475 reflect data that was extracted from that hard drive?
A. Yes.
Q. Like the other devices that you've talked about, have you personally verified that those -- each of these CDs contains data that was on each of those devices?
A. Yes.
MR. CHAKRAVARTY: I'd move to introduce Exhibit 1475, please.
03:46 MR. FICK: Same objection.
THE COURT: All right. Admitted.
(Exhibit No. 1475 received into evidence.)
Q. First I'm going to open 1475-01. What is that?
A. It's the FTK report, the log report that shows the imaging.
Q. Does that reflect that the descriptor for this device was a My Passport, 500 gigabyte USB HDD, or hard drive?
A. Yes.
Q. 1475-02-A, what is that?
03:47 A. It is a complete file listing.
Q. 1475-2-B?
A. Was a derivative file listing.
Q. This is a portion of the --
A. Portion of the complete file listing, yes.
Q. So just looking through this listing, is there -- let's

focus on this one. Is there a foreign-language word followed by a completeinspire.pdf as one of the files?
A. That's the name of the folder that the -- that that would have been on the drive -- on the thumb drive.
Q. So the v-d-o-h-n-o-v-l-y-a-i is a folder name?
A. Yes.
Q. Do you know what that means in Russian?
A. I don't.
Q. But the completeinspire.pdf you've seen before?
03:48 A. Yes.
Q. You've seen that on a variety of the devices that we've gone through today, correct?
A. Yes.
Q. Does this say that it was created on this device at 12/27/2012?
A. Yes.
Q. Does this column have a translation that is consistent with the translations that the linguists at the FBI put on there after they were processed?
03:48 A. Yes. I didn't create that column, but, yes, that's consistent with the other --
Q. As with all of the other CDs that you've described, the translation column is not one that was native on those original electronic media? That's something the linguists did and added to the spreadsheet?

A. Yes.
Q. Were there additional files that you saw on other media, like inspirefall2010.pdf, inspirejanuary2011.pdf, inspiremarch2011.pdf, inspirenovember2010.pdf, inspiresummer2011.pdf, issue9.pdf, jointhecaravan.pdf?
A. Those were consistent with file names that we recognized across several other pieces of data.
Q. And all these files that we've seen throughout your examination today, is that fair to say? The Sheikh Anwar
03:49 Awlaki, Battle of Badr, Sheikh Anwar Awlaki, Battle of Uhud, do you recognize those?
A. I recognize those names, yes.
Q. The files folder on this device, were there -- this is the file structure that was in that folder or partial file structure?
A. Partial file structure that was in that -- on that --
Q. Was there a folder called, "Anwar al-Awlaki lectures"?
A. Yes.
Q. Were Exhibits 1475-04 through 1475-11 in that?
03:50 A. Yes, they were.
Q. Is there a folder marked "tema"?
A. Yes.
Q. Are there foreign-language files in this folder that were actually converted from a proprietary e-book format into a PDF file?

A. I confirmed that these files were resident on the original image.
Q. Was there a folder called "TT" as well, which have more foreign-language files?
A. Yes.
Q. Then there's a folder called v-d-o-h-n-o-v-l-y-a-i that has what appears to be a number of *Inspire* magazines; is that fair to say?
A. Yes.
03:51 Q. 1475-03 is marked "English 2612.docx." Is that a Word document?
A. Appears to be a Word document, yes.
Q. Does that appear to be a submission for English class by someone named Giovanni Norgill (ph), on February 4, 2012?
A. His name is on the document.
Q. Do you know who he is?
A. I do not.
Q. Do you know whether he was a classmate of the defendant's?
A. I do not.
03:52 MR. FICK: Your Honor, I object to the way this one is presented, which I'm seeing for the first time now. As I understand it, if I'm not mistaken, that last file, 1475-03, was actually carved and was not actually in the top structure of the drive. As I see this, I believe it's misleading, so I lodge the objection.

THE COURT: Again, I think it's a matter for your examination.

Q. This external hard drive that you verified the files were on there --

A. Yes.

Q. -- did you export all of the files that you were able to recover from that drive?

A. We -- these files were selected by the team, the investigative team, and we verified that these files existed on the computer.

Q. In fact, were there, on some of these devices, many more audio files and pictures and documents and surf history that we haven't presented?

A. Yes.

Q. Let's go back to the 1R6, the 1142. The *Hereafter Series*, this is a folder and a collection of files that we've seen on some of these other devices; is that fair to say?

A. I recognize the name al-Awlaki, yes.

Q. And this 1142, Sony Vaio laptop, it had several *Inspire* magazines on it; is that fair to say?

A. Yes.

Q. 1142-79, 1142-82, 1142-88, 89, 91, and 93, are all *Inspire* magazines, is that correct?

A. Those are the titles.

Q. In addition, it had a number of audio files that you saw

on all the devices, correct? An example, "Rasool Allah, Inspiring Words of Truth"?
A. You're referring to these here, or which are you referring to?
Q. Yes. I'm sorry. The ones that are in front of you.
A. I would have to actually see them all together. I can't confirm that they were all in all the other places.
Q. And some of these files under the papka folder you found throughout all the other devices; is that fair to say?
03:54 MR. FICK: Objection to the vagueness of the question and the documents speak for themselves.
THE COURT: Sustained.
MR. CHAKRAVARTY: Fair enough.
Q. Do you recognize these files from the thumb drive that was found in the landfill?
MR. FICK: Same objection.
THE COURT: You may answer that.
A. We need to compare the two.
Q. 1150-10 was entitled "completebalance.pdf," is that fair?
03:55 And that is also on the file called -- "complete balance" is also on the --
A. The names are similar, yes -- or the names are the same, yes.
Q. We can do that with a variety of different devices and variety of different files from the 1142, is that accurate?

A. From 1142, from 1R6, yes.
Q. From 1R6, comparing that to a variety of other devices that you talked about?
A. Yes.
Q. I don't need to do that with every one, but I wanted to use that as an example.
MR. CHAKRAVARTY: Just one moment, your Honor.
Your Honor, I believe I'm done. Given that we're at the end of the day, however, I would like -- before I turn it
03:56 over to the -- for cross-examination, I would just ask to hand that baton over on Monday morning.
THE COURT: That's fine. This is as far as we'll go today, jurors, and this week. So we're off for the next three days.
Again, I remind you of all of my cautions, no discussion, no exposure to any media, no independent research. Don't try to educate yourself on computers over the weekend. Your evidence must come here from the courtroom and not from other sources.
03:57 Enjoy the weekend. We'll see you Monday, and we'll continue with the evidence.
(Whereupon, at 3:56 p.m. the trial recessed.)

C E R T I F I C A T E

I certify that the foregoing is a correct transcript of the record of proceedings in the above-entitled matter to the best of my skill and ability.

/s/Cheryl Dahlstrom — March 20, 2015

Cheryl Dahlstrom, RMR, CRR — Dated

Official Court Reporter