sit across the way or what do you want to do?

MS. MARSHALL: I'll move right next to him. He can turn and talk to you.

ARBITRATOR CROW: All right. Mr. McAnn, can you come and take the hot seat, please.

THE WITNESS: Yes, sir.

ARBITRATOR CROW: Thank you.

THE WITNESS: If you don't mind, it will take me a minute to set up.

ARBITRATOR CROW: Take your time. Let's go off the record while he's setting up and you can relax.

(Break taken from 9:17 to 9:25.)

** ** sworn sworn ** **.

Q. BY MS. MARSHALL: You're going to have to speak up into the, speak into the mic and for the benefit of Mr. Crow.

Okay. Mr. McAnn, we've invited you here today to give expert testimony. So I'd like to have you focus your qualifications, your background on your qualifications to assist in making a decision in the issues in this case. I guess let's start with you just describing how would you describe generally your professional work?

A. Okay. My professional work, I have been in the field or fields of IT security, information technology and forensics examinations or forensics for over 13 years. This has gone through both corporate type of cases as well as attorneys, normal litigation and consulting or E discovery. So I've sort of covered the field when it comes to all the different areas where you can apply the forensic back grounds or the forensic services.

Q. Do you, do you have a full time job?

A. I do.

Q. What is that?

A. I have a full time job at a company called *PACR where perform forensic investigations. And this is a corporate environment. Luckily it's flexible so I freelance as well on my own in order to do forensic examinations such as this.

Q. Okay. And the type of examinations that you've done, freelancing, can you give us a general idea of what they are?

A. Freelancing has been from wrongful terminations to sexual harassment, to the stolen IP. So like going through and finding data that a company has, you know, classified or is their own, that

might be going to another data, another company. Excuse me, to fraud, anti trust situations, et cetera.

Q. Okay. You have an idea of how many examinations you've done over the years?

A. Not exactly. Because I do corporate and I do litigation, corporate we've had up to 500 cases a year, which means it can be one computer, it can be three computers that I examine. So I've examined thousands of computers. But I've performed over probably over 500 cases myself. And again that's a cross from corporations type of investigations to litigation type of investigations.

Q. Okay. And you've brought a curriculum vitae with you, which I have a copy for you and for Mr. Crow. And did's a petty detailed CV so I won't have you go through it in detail. But I notice in your CV that you also, in addition to working full time for *PACR and doing consulting that you've just described, that you also are, that you teach the subject.

A. That's correct.

Q. Can you just give Mr. Crow an idea of what your

teaching experience is?

A. So currently, this is the third year I will be teaching advanced forensics, an advanced forensics course at University of Washington. It's a continuing education course and it allows students to go from the beginning, starting with the legal aspect of forensics, through beginner, more immediate to advanced. And so again, I teach the third class, which is the advanced forensics class.

Q. And in connection with your work at the University of Washington, and I see that you've worked at other universities as well, I notice that you have done some writing.

A. I have. Well, I've done writing that I have developed into videos, video tutorials, how to forensics for certain things such as incident sponsor hacking, like compromises on servers to general forensics, et cetera. So I've created at least ten different videos that are posted out on the internet sort of like the U-Tube era for experts such as ourselves to goal study and watch and learn from.

Q. Okay. And have you also been a coauthor of

publication?

A. I'm currently working on an advanced forensics

book along with a person named bill Nelson, who created one of the original or coauthored one of the original forensics books. So it was more beginner to intermediate and he's asked me to help him coauthor an advanced book to be published hopefully sometime next year.

Q. Okay. And I do want you to relate your experience specifically to this case. Can you tell us what types of software and what forensics environments you've worked in?

A. Okay. Well, it's sort of across the board another gambit. I specialize Encase, which has been utilized with some of the other experts here. I specialize in FTK. I also have a lot of knowledge about open systems. So open source software, other software such as X-Ways Forensics, Smart, a lot of different forensic software that's out there. And the reason I do, the reason I'm involved in those is because I have more, I have a lot of experience in not just Windows but UNIX as well as well as

networking and applications. So my, I try to say that I'm the jack of all trades but not quite the master of all or none, I say. Sorry.

Q. Have you, has your testimony been accepted as

expert testimony in federal court, for example?

A. Yes, it has.

Q. Here in Oregon?

A. Here in Oregon.

Q. And when you hold yourself out as an expert, does that include the Windows operating system?

A. Yes, it does.

Q. And are you also familiar with Microsoft Office products?

A. I am.

Q. Including Microsoft Outlook?

A. Very much so, yes.

Q. Okay. So that would include the software that was in use in this case. How about the internet environment?

A. Not only am I an expert, but I've also had training on internet forensics specifically.

Q. Okay. And have you performed in other cases involving issues that involved the deletion of matter or wiping matter or somehow hiding items

in computer environment?

A. As I mentioned, I specialize in what's called incident response. So the compromise of servers by hackers, et cetera, that they love to have a toolset which includes tools that wipe out data,

that hide data. An example would be they may install what's called a root kit that can tell you that you have all of your space available on your hard drive yet you really only have a few gigs free let's say because they're using it to share files out to the entire internet. So I have a lot of experience in that field determining what's been used to hide or wipe data on any source device.

Q. Okay. Now, you were sitting back in the back so you heard me ask questions of the other experts in terms of the concept of technical expert versus a scientific expert. Technical expert being one that can read, can perform the actual forensics, read the machine and tell you what it says, whereas the scientist, the scientific expert being able to take it, a measure beyond that.

Which do you see yourself as?

A. I see myself as the more of the scientist. And the reason that is is because not only do I pay attention to my tools, but I'm eager to reverse engineer what is happening in figuring out why it's happening, et cetera. So that's, therefore, it's more scientific then just

allowing the tool to tell me what it thinks is right.

Q. I would, well, let me ask you one final general background question. I have, I've asked the other experts whether they're willing to testify to the facts in order to help this arbitrator make a decision and I've asked you to do that, the same. Are you comfortable with that as opposed to being an advocate for anyone?

A. Absolutely.

Q. Have you served as a special master before?

A. Yes, I have.

Q. All right. What I'd like you to start with then is to help us understand what the different levels are of metadata. We've talked about metadata so far, but I don't know that anybody has educated us as to what it is.

A. Okay. Well, I'm going to keep it limited to the involvement of this case. But basically and I think I have heard someone here, someone of the experts say this metadata is usually data about data. It's kind of confusing. However there's two levels in this case there's file system metadata. File system metadata means the name of the file, the times, the times that

Mr. Williams was talking about earlier that may or may not change. That's file system metadata. And then there's application metadata. And that is like if you have your Microsoft Office, you open up a Word document, you know, your Word document stores things like the author, the company, how many words or characters are in the document itself when it was last printed, et cetera. There's a lot of data that's stored within the document itself, which becomes --

ARBITRATOR CROW: Is he going too fast for you? Are you okay?

THE WITNESS: Am I going to fast for you, sir?

ARBITRATOR CROW: No. No. I'm more

concerned with those fingers over here. Go ahead.

THE WITNESS: So the document contains metadata itself, which again corroborate with the file system metadata as we will probably be explaining later.

Q. BY MS. MARSHALL: Okay.

ARBITRATOR CROW: I understand.

Q. BY MS. MARSHALL: Whereas here, one of the pivotal issues is the date, date and time. How

can the metadata help us to figure out the actual date and time, not just read it off a machine, but to figure out the actual date that a document was created or a file was created?

A. Well, the metadata both file system and application metadata can have and will have a created date and several other dates involved. You can try to --

ARBITRATOR CROW: On the document itself?

THE WITNESS: On the document itself if we are referring to a document, which we are during this case, and on the file system. So usually you would refer to those two different metadatas for the dates and times in order to depend on

them.

ARBITRATOR CROW: Well, let's take a look at Exhibit 146, which I think is the last one. I need to make sure I understand what you're talking about. You say there's a creation date. I only see a creation date on this document. Would there be another date that you would find and where would you find it if you did.

THE WITNESS: Which page?

ARBITRATOR CROW: Page two, for instance. This e-mail is apparently sent October 1, 2003,

at 9:35 a.m.

THE WITNESS: So in this case this is an application metadata date. Right. And this is actually called, if in some of the reports from Steve Williams this is technically the submit metadata that the date in which they actually punched that send button. Do you mind if I show you on the screen?

ARBITRATOR CROW: No. That would be fine. And if you would like to come down.

THE WITNESS: You will all recognize this. I'm not going to actually send it. But I am

going to create a new e-mail and this is Outlook. This is also, I should mention that this computer is tuned so it's Outlook XP, office XP just like what existed when this data happened when all the data was being utilized.

So, the submit time or the sent date is the actual time when they go up here and they click on this send button.

ARBITRATOR CROW: That's the date that would be on this document that I just referred to.

THE WITNESS: That is correct.

ARBITRATOR CROW: All right.

THE WITNESS: Now there's other application

metadata for this office Outlook application. So there's created which you don't see here as well as received and last modified. So there's four dates that off Microsoft Office Outlook has.

ARBITRATOR CROW: And are you able to extract those dates?

THE WITNESS: Yes.

ARBITRATOR CROW: From the computer?

THE WITNESS: Yes, I am.

ARBITRATOR CROW: The hard drive; is that

correct?

THE WITNESS: Yes, sir.

ARBITRATOR CROW: Okay. I think I understand where you're going.

Go ahead.

Q. BY MS. MARSHALL: Okay. Now, are there ways, once you have these four pieces of metadata, are there ways that you can test them to verify that, in fact, they are true, are the truth?

A. Well, the best way, forensically, to test to make sure that these dates are the truth is by comparing them with computer log files, you know, to make sure that at no time the computer date was changed. I can demonstrate this as

well if you'd all like to come back up.

Q. Let's wait until we get a little bit later and then he can do it all at once.

ARBITRATOR CROW: Are you saying there is a way to look at the hard drive to see when and if a date was changed manually?

THE WITNESS: Yes, sir.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: Okay. And what would you look

at on the hard drive to determine if a date had been changed?

A. Again I would look at different log files that existed on the hard drive.

Q. And do you have to have the hard drive in order to do that?

A. No. When it comes to e-mail anyway, e-mail you could also refer to the internet service provider that the e-mail went through if the e-mail went through an internet service provider.

Q. Okay. With respect to a paper document, for example, the letter that's at issue in this case, would you have to refer to the hard drive in order to examine the logs?

A. Yes.

Q. Okay.

ARBITRATOR CROW: Give me that one again, Linda, that question again.

Q. BY MS. MARSHALL: I asked whether with respect to the written document, the letter in this case, would he have to examine the hard drive in order to, examine the logs on the hard drive in order to verify the date and time?

ARBITRATOR CROW: And the answer is no?

THE WITNESS: To, since she, since she clarified the question, the answer is that log files, I utilize log files to validate dates and times. But to validate an actual date and time from a piece of paper that was printed or used on a computer, then I have to go into the file system and the applications and configuration on the hard system. So the hard drive is the answer is yes, I absolutely need the hard drive to validate that document.

ARBITRATOR CROW: All right. Thank you.

Q. BY MS. MARSHALL: Okay. Now, you've been in this field for 13 or so years. I want you to focus on the period 2003, 2004. I've asked you to do this in this exercise at least. Do you have an understanding of the concept of a

litigation hold?

A. Absolutely. So a litigation hold is where one or both parties understands that litigation is going to be occurring and whatever the allegations are, any evidence involved in that litigation must be held, meaning it must be set

aside and untouched during the time of that litigation.

Q. Okay. And are you talking about taking computers out of service?

A. Not necessarily. You could take the data storage devices out of the computers and replace them and still have them in a running, in the business or the company or whatever it may be and have those data storage devices out as the evidence that you need or the, yeah, the evidence that you need, that you are holding for the litigation.

ARBITRATOR CROW: Can you take a mirror image at that time and preserve it?

THE WITNESS: Yes, you could.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: Okay. And that would be by the parties getting together and agreeing that they would hire somebody together to take an

image; is that correct?

A. That is correct.

Q. Okay. Now, what about a litigation hold with respect to storage devices like floppy disks and things of that nature?

A. The same applies to any sort of data storage device, whether it's a floppy disk or a CD rom, the idea is that it is stored and it is not touched in a technically it's not touched as in no one wrote to it or no one has modified it or corrupted it.

Q. Okay. And in 2003, was it your understanding that this was the practice in the industry that when litigation was imminent, that a litigation hold as you've described it would go into effect?

A. While E discovery was new in 2003, I was performing this exact role in my life. And so yes, it was still common practice for that to be in place.

Q. All right. And as a forensic examiner, are you familiar with concept of spoliation?

A. Yes. So spoliation is the intentional or even unintentional change or manipulation of data that may be in that litigation hold. It could

be the accidental deletion of a file, it could be the accidental overwritten file or it could be the loss of data or the loss of a data

storage device itself.

Q. Okay. And have those sorts of things happened in this case?

A. Yes, they have.

Q. In your course in advanced forensics, do you teach your students about litigation holds?

A. Absolutely.

Q. Do you teach them about spoliation?

A. Yes.

Q. Have you found examples of spoliation in this case?

A. Yes, I have.

Q. And have they put Mr. Zweizig at a disadvantage?

A. Yes, they have.

Q. Okay. You spoke a moment ago about your, the computer that you're using here today, that it is loaded with the same software that was in use in 2003 by Mr. Zweizig's computer; is that correct?

A. And Mr. Rote's.

Q. And Mr. Rote's computer.

A. Yes.

Q. Do you have available to you the forensic tools that were available? For example, the ones that

Mr. Williams was using?

A. Yes, I do. Although they are, they have newer versions out and newer capabilities than Mr. Williams had back in 2004 and 2005 when he took his images and did his analysis.

Q. Okay. And so have you attempted to use the newer versions of the forensic tools?

A. Yes, I have.

Q. Okay. But I would like, whenever possible, when you're talking about, when you're trying to compare your data with that, that either of the other two gentlemen has used, that if you could refer to the same forensic tool, whether it be --

A. Newer or not.

Q. No. Whether it be Encase or FTK. Is it FTK?

A. You got it. Correct.

Q. Maybe you could explain for Mr. Crow the difference between those two.

A. So let's start with FTK.

ARBITRATOR CROW: D or --

THE WITNESS: T. It stands for forensic tool kit. It was really developed to sort of

more towards the technician side of a forensic examiner, which means that it takes all of the data in and processes it first and then spits it out in buckets. This is how many documents you have this is how many e-mails you have this is how many spreadsheets you have type of scenario. So it's very commonly used or most commonly used I should say with law enforcement. The other product that has been used in this case is called Encase. That's E N C A S E. That product is, in my opinion, more advanced than the FTK product, means that you open up your case, you are looking directly at your data storage device and you have to work through it similar to sometimes to a hex editor. So it can get very complicated.

Q. Okay. The demonstrations that you've brought here today, are you going to be permitting Mr. Crow to actually look into the FTK and the Encase and what was the other thing, the hex editor?

A. It's called X-Ways forensics and that one is not loaded on here because I did not use it during this case. However, if absolutely at any time it pops up in my examples I will be showing you

both of those products.
Q. Okay. I'd like to have, I'd like to move right into one of the, one of the important issues in the case, and that's the e-mail that's at issue. And I believe it's Exhibit 14. I'll let you take a look at it. And I'll just ask you whether I have asked you to do forensic examination with respect to the, to this e-mail.
A. Only in respect to the latest protective order.
Q. Yes.
A. Have I taken a look at this e-mail and examined it forensically.
Q. Okay.
A. I'm sorry. Let me add onto that. The prior, the prior stipulation, protective order, I found this e-mail but it wasn't in the stipulation for me to really bring it out and examine it fully like I have since the new protective order came out.
Q. Okay. Well, let's go back to the first time that you approached the subject of the e-mail. And first of all, what computer did you understand the e-mail was created on?
A. My understanding is it was created on Mr. Rote's laptop.

Q. Okay. And were you provided Mr. Rote's laptop for examination?
A. Yes, I was.
Q. Okay. When were you provided his laptop?
A. I believe it was December 12th, 2008. And if you don't mind, I'm going to grab my folder down there.
ARBITRATOR CROW: December 8th?
THE WITNESS: Yes.
MS. MARSHALL: December 12, 2008.
THE WITNESS: I am going to refer to, for this I am going to refer to my report that I submitted. I don't know which exhibit it is.
MS. MARSHALL: It is an exhibit, I believe. While you get it out I'll get the report number.
THE WITNESS: So to continue with that, I was, I was, did you handed over?
Q. BY MS. MARSHALL: You were provided. Were you provided the actual laptop?
A. I was provided the actual laptop on December 12th, 2008.
Q. Okay. And the date of the e-mail is what?
A. October 2nd, 2003.
Q. Okay. So you were looking at the forensic data

roughly five years after the, ostensibly after

the e-mail?

A. Can you repeat the question, please.

Q. I guess I was just summarizing that you were looking at the computer roughly five years after October of 2003.

A. That is correct.

Q. And where were you, where were you, where did you go to get the computer?

A. I was actually in this building. I can't tell you which floor, but, or which law firm it was, but the name of the attorney was Jeff Edelson.

Q. Okay. So you, your office is in Seattle?

A. Yes.

Q. Is that correct? So you came down here specifically to examine or to take images of the relevant computers?

A. That is correct.

Q. Okay. Can you tell us the general condition of the laptop at that point?

A. The laptop physically did not look damaged.

Q. And what did you find when you went to take an image of it?

A. What I found is that the hard drive itself,

however, did appear physically damaged, not from the outside but by the sounds and its

performance that it had when I was attempting to take a forensic image, such as whining and almost a grinding sound inside a hard drive, smug would hopefully never want to hear unless you backed up all of your files.

Q. Okay. We should have probably done this earlier, but when you say you take an image, what are you really talking about?

A. So what that means, and actually I'm going to grab my bag for this. What that means is that there's a procedure, procedure that I utilize in order to preserve the evidence. And this procedure first off starts off with me documenting what the evidence is and the documentation comes in three forms. It comes in writing it down, as an example. I have these forms that I fill out when I go on site and I actually look at the equipment and take the equipment. So I'm writing down serial numbers and model numbers, et cetera. The second is the chain of custody. And the third is actual

pictures. So I take a camera along with me and take pictures. Equipment so I can tell what state it was in, I can tell how it was configured and I take up close macro shots of

the serial numbers. This is how I keep from accidentally not being able to read my own handwriting.

Q. All right. So when you say an image, now the other two gentlemen have talked about images, too. What is, what is an image?

A. So after I have documented everything that I need to, that I feel that I need to, I do what's called a forensic image, taking a forensic image. It's a bit by bit or byte by byte, depends on how you want to say it, copy of a data storage device. And that data storage device can be a hard drive or a floppy disk or a CD rom or anything. It can be an i-Pod or what's inside an i-Pod I should say. So what happens is that most of the scenarios, especially computers and with their hard drives, we hook them up to what's called a write-blocker device. It's a piece of hardware. And the reason why we use a piece of hardware is as to

things like viruses don't affect us. If my computer here gets affected and I'm suing a software device in order to keep from writing to a hard drive, it's possible that that virus has taken over and changed it to where I can

accidentally contaminate my evidence. So that's why us in the field use hardware write-blocker devices. Once we attach the hardware write-blocker device to the data storage device, then we have a target data storage device usually an external hard drive which we have wiped, meaning we've wiped it completely clean. So even us forensic guys can't go and recover anything off of it. It looks like just a bunch of zeros. And then we begin to take our forensic image copy from the source off to our target drive and that's how, where we make our images.

Q. So the net result is that the objective is that everything, every one and zero, if you will, on the, whatever you're taking an image of, ends up on your external drive, is that --

A. That's correct.

Q. Is that it?

Okay. And then you give the original back to its owner?

A. That is also correct.

Q. Okay. Does that relief the, is your understanding that that relieves the owner from litigation hold?

A. No.

Q. Or from taking it out of service, et cetera?

A. No. And I say that only because you never know what the next request may be. As an example, this may not apply to this scenario, but when it comes especially to either discovery, I may be asked to search this entire data storage device for certain keywords. Right. And then three months down the road they may come back and tell me that I need to go back to the hard drive and pull more data off it in order to additional keywords to that.

Q. Okay. When you went to take your image of Mr. Rote's laptop, were you able to get a complete bit stream image of that laptop?

A. I was able to complete the image after multiple tries, since it was physically damaged, and,

however, the software that we utilize goes through and if it has trouble reading any part of the drive, it records it but it marks it all as zeros. So I can't actually get access to the data, wherever those bad areas were. And again, I actually tried imaging this drive five times during the course of the period that I was at this, at Jeff Edelson's office.

ARBITRATOR CROW: The laptop.

THE WITNESS: Of the laptop, yes. Whereas each one almost took an hour to complete. The size of this drive was ten gigabytes. It really should have took maybe 20 minutes. So there were issues and the image that I received, even though it was a, even though the software completed, I did not have access to all of the data on that 10 gigabyte hard drive.

Q. BY MS. MARSHALL: Okay. Now, if, we've talked about the litigation hold. But let's say the computer is not taken out of service. So the hard drive is not taken out of service. What effect does that have on the forensic evidence?

A. The longer and longer that hard drive or data

storage device is kept in service, the more data that is deleted is overwritten. You know, the more it fills up, the less of a chance you have of recovering deleted files.

ARBITRATOR CROW: And if it's overwritten, you can't recover it?

THE WITNESS: That is correct.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: With any of your tools; is that correct?

A. That is also correct. Without it being sent off to a science lab.

Q. Okay. Now, the corruption on the laptop, did it affect your ability to read the registry?

A. Yes. Yes. I was unable to read the registry or even the backup registries that the computer automatically takes.

Q. Okay. Could you tell whether the laptop had been in use during the five years since October of 2003?

A. Referring back to my report.

Q. The report is Exhibit 103, Mr. Crow. We've located it down here. It is in evidence, I believe.

ARBITRATOR CROW: I think it is.

THE WITNESS: What's the third page on that? Is it 103, page 3?

Q. BY MS. MARSHALL: 103, Exhibit 103, page three. Okay.

A. Yeah. I believe if it's going based on this. I wrote in the, on the sort of second paragraph on that page, the very, the second to the last sentence talks about how this 10 gigabyte hard drive has been in use since the termination of Max through 11-12-08. So exactly a month before

I took the image and I had this in my hands.

Q. BY MS. MARSHALL: Okay. In your judgment when should the litigation hold have gone into effect for the hard drive that this exit time e-mail was created on?

A. In my opinion, the moment whomever initiated the litigation, you know, began to think about the litigation and/or discuss the litigation with an attorney.

Q. Okay. And is this an example of what you were talking earlier about, spoliation, what can happen if the litigation hold is not put into

effect?
A. Absolutely. The fact that these were in use for years arch the litigation was put into effect is unintentionally overwriting data, which is spoliation.
Q. Did it prevent you from doing what you needed to do in order to properly examine the hard drive for this e-mail?
A. In several instances. A lot of, especially if we're talking about just the e-mail, this e-mail that was, to exist, you know, it's possible that copies or original drafts, et cetera, existed on this laptop at one time but I was unable to

discover because of the overwritten data.
ARBITRATOR CROW: Well, let me ask you this, as I understand your earlier testimony, you can determine from the hard drive whether the date on the computer has been manually changed.
THE WITNESS: That is true.
ARBITRATOR CROW: Can that information be overwritten?
THE WITNESS: Absolutely.
ARBITRATOR CROW: All right.
THE WITNESS: Log files generally will do

what they call role over. So they can only go, get up to a certain size and then after that size is met, then they start overwriting the date a that's in the beginning it. It's also very similar to how the hard drive works when it deletes data.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: And in your view did that put Mr. Zweizig at a disadvantage?

A. Yes, it did.

Q. Fortunately you have had access to, now, to an earlier image of the laptop; is that correct?

A. Yes, I have.

Q. You were, after Mr. Williams testified and you

obtained his file, you were given an image that he created in May of 2005?

A. June of 2005.

Q. June of 2005. And have you had -- When was that that you were given access to that?

A. That was actually last week, last Tuesday. And the date skips my mind. So you'll have to fill that in for me. Actually I can fill it in. Tuesday, October 26th.

ARBITRATOR CROW: Okay. You examined it --

THE WITNESS: No. I received it.

ARBITRATOR CROW: All right. And this is an image taken in June 2005.

THE WITNESS: By Steve Williams.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: So this is 2010 and we're in the middle of the arbitration. And is this the first time that you have been able to examine the computer as it was in 2005?

A. Yes.

Q. And even then it was a year and a half after the fact; is that correct?

A. That is correct.

Q. Okay. And first of all, did receiving this image, even though you now have it, did that, in

your view did that put Mr. Zweizig at a disadvantage?

A. Yes, because that year and a half is still, and the fact that the drive is so small, being a 10 gigabyte drive, that far back, the data that's being overwritten happens even faster than a drive that is bigger.

Q. Okay. So when you examined Mr. Williams' image

of the laptop, did you find missing or data that was, or did you find that data was missing that you would have hoped to have seen there?

A. Are you asking did I find data that I didn't find when I took my own image?

Q. Let me rephrase the question. Did you, in looking at the image of the laptop that Mr. Williams took, was there data missing that you would have hoped to have seen that you attribute to overwriting, et cetera?

A. One example, and there are many more, would be the log files. The idea is that, when I originally had access to this computer, not only was there an e-mail, you know, or e-mails about the termination, but there was a letter about the termination. And I was unable to find that information on the computer. That was before

Mr. Rote's testimony. And I was unable to determine if any of the dates were modified or manipulated because well even a year and a half later that data is, has most likely been overwritten.

ARBITRATOR CROW: Well, to overwrite at the

change of a date, manually, would you have to manually change the date? I mean, is that, do you overwrite the change of a date by change being the date again.

THE WITNESS: Yes, you can.

ARBITRATOR CROW: Is that the only thing that would overwrite the change of a date?

THE WITNESS: No.

ARBITRATOR CROW: What else would.

THE WITNESS: There are programs that can.

ARBITRATOR CROW: All right. Go ahead.

Q. BY MS. MARSHALL: Okay. In addition to examining Mr. Williams' forensic image, which I take it you're primarily relying upon now; is that correct?

A. As of a few days ago, yes.

Q. Okay. Did you review his report?

A. Yes, I did.

Q. Okay. And that would be Exhibit 68. And we

will be referring to that quite a bit?

ARBITRATOR CROW: 68?

MS. MARSHALL: Exhibit 68, is a report that Mr. Williams prepared in 2005 relating to his examination of the laptop.

Q. BY MS. MARSHALL: Let's see. You need to have Exhibit 68 in front of you. And we have the books down here, I guess.

A. Is it okay if I pull it up on my computer instead?

Q. Sure. If you have that on your computer, that's fine?

A. I believe that was Exhibit 5, NWD 0005 before; right?

Q. Yes. Okay. Let's start with the general first and then move toward the specific. And here, I think you'll be able to make some demonstrations for us. But basically what I want to know is how difficult it is to manipulate the date and time on a computer?

A. It is not difficult at all. It's easy enough that even a general user just first buys their computer can do it. Would you like a demonstration?

ARBITRATOR CROW: Would I do it the same as

I would change the time, use that same?

THE WITNESS: Simply by double clicking on the clock in the corner, that's exactly how you

change the date.

ARBITRATOR CROW: Okay. I've had to change the time so I understand how it's done.

Q. BY MS. MARSHALL: Okay. Now, when you do that, how does that affect the metadata in the computer?

A. That actually will change, not necessarily change, but that will impact the file system metadata as well as the document metadata. As an example, the dates and times that we're looking at in this exhibit, that's application metadata. That's metadata that Outlook, Microsoft Outlook has put into this e-mail. So by changing a date you could, well I mean demonstrate this. And I already have, in a way, if I change my date from right now I actually have it dated until tomorrow. Let's say I change it to November 1st of this year, this month, okay, I set my date back just by double clicking as you are aware of changing your time, correct. Now whenever I, if I create a new e-mail and I can make this to anybody, I'll send

it to Max, what was it Erols, E R O L S. I think I spelled it wrong but it doesn't matter.

Test e-mail. All right.

Q. Now, before you go any further, can I ask you, do you have to be hooked up to an internet in order for this to, this demonstration to work?

A. No.

Q. Okay. So you're not depending on any outside. So this is all within the computer; is that right?

A. That's correct.

Q. Okay. So why don't you show us what happens to the date and time that you just made the change to.

A. Okay. Once I send this, it's going to write a couple different dates, three different dates actually. It's going to write creation date, a receive date and what's called a sent date or a submit date. The submit date actually will not happen because as you can see here it is sitting in my out box. But it will have a fourth date called a modification date. And that you will see back on the exhibit, so what I just did is going to create this creation date, a delivery date and pay a modification date.

ARBITRATOR CROW: But not a submit date.

THE WITNESS: Not a submit date. Not yet.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: Well, let's just back up to the creation date.

A. Okay.

Q. What starts the creation date? What button do you hit that starts the creation date?

A. New e-mail. So the new button in your Microsoft Outlook.

Q. Okay. So that's the creation date and time; is that correct?

A. Yes.

Q. For the metadata. And what creates or what starts the delivery date and time?

A. It's actually part of the send, once you send it, there's a send where it sort of saves it. You could call it save it in memory or a queue. Let's call it a queue. It's a place in line. All right. Once that gets, even though you hit the send button it's not officially sent, it's not officially submitted. It still has a receive time of when it sits in that queue and waits for it to be officially submitted.

Q. Okay. And would that also include, if it was

saved?
A. Yes.
Q. Okay. So if you save it rather than, if you don't, let's say you don't send it at all, you close and it asks you do you want to save it and you say yes, that would, that would create a delivery date also?
A. Yes.
Q. Okay. Now, there's some discussion about this submit date. Okay. And as to whether that is when somehow the e-mail bounces off of an ISP or something like that. And you recall Mr. Williams' testimony about that?
A. Mr. Williams' testimony was he thought that the submit date was received back from the server, like a response once you send it out. In truth, the submit date is put into place the same as automatic the other dates by the application, not by the outside ISP or a server of some sort, for the sender. I want to be specific. That's for the sender. It does not receive that send date or that submit date by an ISP. A recipient, however, a recipient of that e-mail will receive a date, one of these dates will be changed and applied by an ISP. But in this case

all we're dealing with, all of our exhibit is dealing with is the sender, sending out the information or the e-mail.

Q. Okay. And how did you figure that out?

A. Well, besides being an expert and I have a lot of experience with these applications, I put the scenario into play. You know, I have created a computer, a lot top, very similar to Mr. Rote with the same software, the same name built into, and same company, et cetera. So when I send it out, whoever I send it to, it delivers the date back that I just set the clock to. I've tested it multiple times.

ARBITRATOR CROW: Well, I understand that. So you can change the date on your own computer.

THE WITNESS: Uh-huh.

ARBITRATOR CROW: But as far as the received time is concerned, it's going to show the actual date of receipt.

THE WITNESS: Only on the recipient side.

ARBITRATOR CROW: On the recipient side. I understand that. So have you examined Mr. Zweizig's computer to see when he received that e-mail?

THE WITNESS: Yes. And both, I should say.

ARBITRATOR CROW: All right. Am I getting ahead of things? I'm sorry.

MS. MARSHALL: Yes.

ARBITRATOR CROW: I apologize.

Q. BY MS. MARSHALL: Okay. So in terms of the metadata that's shown on Mr. Williams' report, the creation, the delivery, the submit dates, all October 2nd, 2003, is there anyway to decide whether those are the true dates given the fact that you've now created an e-mail that, or can you create an e-mail that, today that has an October 2nd, 2003, metadata in it?

A. Yes, I can.

ARBITRATOR CROW: I assume you can.

Q. BY MS. MARSHALL: So now that you've shown us that you can do that as a forensic examiner, is there a way you can get around it and figure out whether that has been done?

A. And the only true way of doing that forensically is by being able to analyze logs to seem if the changes were ever made. And if you don't mind I'm going to demonstrate this as well. I've changed my date on this computer several times.

And I happen to be logging my firewall, the network. So the network connectivity that's

been going on with this laptop since I've been at home, since I've been here on the wireless network here, it's been logging to a log file on my desk top here. And this log file is the firewall log file. What you are going to see here say log file writes sequentially. It doesn't care what the date is. It doesn't care anything. It's going to keep writing it one line by line. And it doesn't sort by anything. So as you change your date you'll notice, I'm going to light it up here, you'll notice that I went from 10-26-2010 to 10-26-2003 back to 10-26-2010. Right. That's, so I can tell when, by analyzing log files when somebody changed their date and time. And I mean, and you see this log file is very big, but you can see that the changes are still there and it, again, you'll see I went from here 10-05, October 5th, 2010, to October 5th, 2003. It doesn't have to be just a year. It can be any date any time that I change and I will see the difference in a

log file.

Q. Okay. And with a 10 gigabyte hard drive, which is what the laptop had in it, would you be able to look at the logs and determine whether

anybody had, during that period of October of 2003, say, through October, or through May of 2005, whether anybody had tampered with the internal clock?

A. Only if I get to the log files in time. Before they get overwritten. This one happens to be set for 32 megabytes. So after it's written 32 megabytes, it's going to start to overwrite everything in the beginning. Most of them by default, this is only set to four megabytes. So after a long time, especially with a 10 gigabyte drive, this information will get overwritten before I got a chance to examine it.

Q. Okay. Are there any other ways that you can try to test the, whether something has happened to the date to make it less reliable, other than the logs? And I guess I'm thinking of files, file paths, I guess what I call them. Maybe I'm, maybe I've got the wrong name.

A. Yes. An example would be usage. If you were

going to do an investigation about the activity on a computer, I don't know if we can find it, but in one of the exhibits that Steve Williams has wrote in his report, he shows a timetable that Encase is able to produce. So it shows

that on yesterday so many files were written to, so many files were accessed, so many files were modified, et cetera. All right. So many files were created. It's a timetable in one of his exhibits and I don't know which one or if we have the ability to find it quickly. However, that timetable can say, let's say if you have, I wish we could draw here. If you have a square for a day of every week, let's look at the squares on this wall. Okay. So we have and we'll count that one as seven over there. All right. So if you have a square and this is a big timetable of each one in the seven days in it, you know, if something is empty, if one of these squares is empty, then in a timetable the assumption is if the square is empty that the computer was not accessed or turned on during that day. And that's another way you can go

through and identify --

Q. If something happened?

A. If anything happened.

Q. Okay. Let's go back to Mr. Williams' report, Exhibit 68. The last, the fourth bit of, I hate to say bit, I shouldn't say bit, should I. I should say the fourth piece of metadata, the

modification date is April 29th, 2005, at 6:00 p.m. did that catch your attention?

A. Yes, it did.

Q. And did you --

ARBITRATOR CROW: The image was taken on June.

THE WITNESS: Fifth.

ARBITRATOR CROW: 2005. Okay. Go ahead.

Q. BY MS. MARSHALL: That's roughly a month before the computer was given to Mr. Williams to examine.

A. He examined it on, well he took the image on June 5th, 2005.

Q. Okay. And this modification shows that it was modified on April 29th, 2005. Now, you were here when Mr. Williams explained that he had called Mr. Rote and asked for an explanation.

A. Yes, I was.
Q. And the explanation was that he had moved the e-mail from one folder to another.
A. That's correct.
Q. Is that an acceptable explanation for you?
A. No.
Q. Why not?
A. Because even moving a, an e-mail from one area

on what's called a PST file, let's say you can see your e-mail when you open up Outlook. Right. But let's say you want to save it to a back up file, a back up place where you just store everything because you just, you're so busy and you have all these different cases that you have another area such as, such as an archive, right, where maybe in this archive I want to create a new folder, which is NDT versus Zweizig. And then in this folder I am going to go to my normal in box or wherever I want, wherever they come in and I am going to move these files, not these files, but these e-mails to a back up. Okay. Well, just by moving it to this back up from here, it does not change the

modification date of this e-mail. And even if I moved it from this location to old cases. All right. So now even if I moved it from this location in this archive to the next one, it actually does not change the modification date which was the assumption of Mr. Williams when he gave his testimony.

So again, by being more of the scientist and by not only know this program, but going and doing multiple tests in cases to verify this

data, I can verify that it moves from one to the other, even from one archive to another archive, basically two different files and the modification date will not change. The only way or --

Q. Let me ask you, what will change the last modified date, the modification date?

A. The only way that you can change the last modification date or the only way that the normal users of a computer will change the modification date is by opening up the file and I believe Williams in his testimony said that I can't really modify an e-mail. Well the truth is that within Outlook itself, if you go to

edit, you'll see right here, once you've sent it, whether it's sent, whether it's here whether it's in your send mail or drafts, wherever you have this e-mail sitting, if you open it up and go to edit and edit message, then you can change, you can change the body of the e-mail and you can change the subject of the e-mail, et cetera. And once you change it, so if I change it --

Q. Let me ask you again, can you change the to and the from?

A. No.

Q. And you can't change the date this way?

A. No, you cannot.

ARBITRATOR CROW: Can you change the creation date.

THE WITNESS: No. So the only thing that changes even by simply erasing this period on the end of this sentence, right, and then I quit and it asked me do I want to save it, now I just changed the modification date to whatever the date is set on my computer.

Q. BY MS. MARSHALL: Okay. So if that's not the

answer to why that modification date is April 29th, 2005, did you look into it further to see what the answer is?

A. I think you might have to reclarify that question.

Q. Did you examine the image of the laptop further to try and figure out what happened on April 29th, 2005, 1 month before it went to Mr. Williams?

A. I did. And, again, as I was explaining with the squares on the wall, there was no activity on the computer from a file metadata perspective. There was no activity on the computer at all on

April, April --

ARBITRATOR CROW: 29th.

THE WITNESS: April 29th, 2005.

Q. BY MS. MARSHALL: What does that tell you?

A. That tells me that either it wasn't used on that date at all or the information that would tell me has been overwritten because of the time that's passed between when it was actually used and the time I got to examine it.

Q. Okay. So if we're looking at the blocks on the wall here, April 29th was a Thursday, as I

recall; right?
A. Yes.
Q. So that block would be blank on the, in what you call the file system?
A. Yes.
Q. Nothing there at all as if the computer hadn't even been opened?
A. That's correct.
Q. Okay. Did you go looking for the e-mail, the exit time e-mail?
A. Yes, I did.
Q. Did you find it?
A. On --
Q. April 29th.

A. On which data storage device?
Q. On the laptop, on Mr. Rote's laptop?
A. I did find it on the, on Mr. Rote's laptop.
Q. Okay.
A. I found the same e-mail that Steve Williams found in his report.
Q. Okay. And I should be referring to when I'm talking now, you're using Mr. Williams' forensic image and you're using the same forensic tool

that he was using; is that correct?

A. Two things. When I originally examined the hard drive or the laptop from wrote's, when he gave it to me on December 12th of 2008, I was able to find the exit time e-mail on his hard drive. I was not able to find it at all on any of the two drives supplied by or supposedly owned by Max Zweizig.

Q. Okay.

A. And I was not able to see any activity on the four 29 on either my image that was taken in 2008, December 2008, or on the one provided by Zweizig, I mean, sorry, Steve Williams and Mark Cox.

Q. Okay. And have you now found information related to the exit time e-mail on April 29th,

2005?

A. Repeat that.

Q. Okay. Well, tell us what you have found with respect to, what happened on April 29th, 2005, with respect to the exit time e-mail?

A. Nothing that I can find.

Q. Okay. Did you find more than one version of the exit time e-mail?

A. No, I haven't.
Q. All right. Did you find an exit time e-mail in deleted space?
A. Yes.
Q. Okay.
A. Yes.
Q. Tell us what you found.
A. So in the image that was provided to me by Mark Cox, which happens to be the image taken by Steve Williams, I found another exit time e-mail, actually we're looking at it right now, another exit time e-mail that was forwarded to, I will put my hand right below it. I found an exit time e-mail the same one that was forwarded to a Ryan Burglahaus, House, not sure how to pronounce it, but that was actually done on which date? On the 29th, 2005. The almost

exact same time as this e-mail was supposedly sent to Max Zweizig or at least not, I'm sorry, that was incorrect. Almost the same exact time as it was stated that this was sent. You know, however, this --
Q. Modified?

A. Modified.
Q. So in the image, and I may have been confusing you because I didn't realize that you were looking at Mr., at the image Mr. Cox had provided you.
A. I have not been provided the evidence or images that Steve Williams has really had his hands on or been working on. I only have been provided the, I can't remember what you call it, but the code or the evidence that Mark Cox has been provided.
Q. All right. Then I'll refer to that. So in that forensic image you found two copies of the exit time e-mail, one with the metadata that's shown in Mr. Williams' report, the other that had been deleted on April 29th, 2005. Did the one that had been deleted, did it have the same metadata as the one that's shown in the report, create date, delivery date, et cetera?

A. It only had the same modification date and time.
Q. Okay. And did you look at that e-mail to see if it was the same e-mail? Was it an exit time e-mail?
A. It was an exit time e-mail. But the created and

sent date, everything except for the last modified, modification time was the same. The modification time was different though, I'm sorry, received and sent dates were different. They did not match.

Q. Is that the one you have up there?

A. Yeah. This is the one that was different, yes.

Q. Okay.

ARBITRATOR CROW: This is the modification that has the different date?

THE WITNESS: Yes.

ARBITRATOR CROW: From sent and received? All right. It was sent on April 29th, 2005?

THE WITNESS: Correct.

ARBITRATOR CROW: Okay.

Q. BY MS. MARSHALL: So can you take us any further into what really happened on April 29th, 2005? To this e-mail?

A. No.

Q. Okay. Normally if you had, if you had the image

and time, you would be able to go to the file system and see what happened there. But that's blank.

A. Yes.
Q. As if nothing it happened?
A. Correct.
Q. When, in fact, we know something did happen.
A. Correct.
Q. Now --
ARBITRATOR CROW: So you can't tell us what the modification was, if there was a modification, whether it was a change in date or anything of the sort, is that what I'm hearing?
THE WITNESS: Yes.
ARBITRATOR CROW: So there was a modification but you can't tell us what that modification was.
THE WITNESS: That's correct.
ARBITRATOR CROW: And there may have been no modification at all, but simply a transfer of the e-mail from one place to another; is that correct?
THE WITNESS: That's correct.
Q. BY MS. MARSHALL: Well, now wait a minute. That last part, is that really correct, if it was

just, if the e-mail was just transferred from one folder to another, would that change the

modification date? I thought you had testified about that earlier.

A. Can you repeat that question?

Q. Okay. If, as Mr. Rote testified, he simply moved the e-mail from one folder to another, does that change the modification date?

ARBITRATOR CROW: Does it create a modification date, I think is the question.

Q. BY MS. MARSHALL: Well that might be the question, too.

A. Yes. I mean, if, if you simply have changed it or moved it, you know, that date will have changed.

ARBITRATOR CROW: Well, as I understand it, on April 29th, 2005, this e-mail was sent from someone whose name I don't recall or to someone whose name I don't recall. Would that create a modification date if everything else was the same on the e-mail?

THE WITNESS: Yes.

Q. BY MS. MARSHALL: Okay. So I don't want to confuse it any further.

A. Okay.

Q. When Mr. Rote said that his explanation being that he simply moved the e-mail from one folder to another folder, and I thought you testified that that did not explain the change, the modification date. Have you tested that?
A. Yes, I have.
Q. Okay. So now what you're saying is that if it were forwarded on that date, that would change the modification date?
A. That's correct.
Q. Okay. Did you find that it was also deleted on that date?
A. Yes.
Q. Would that change the modification date?
A. I don't know.
Q. Fair enough. Because there were two e-mails; is that correct?
A. That's correct.
Q. Okay. In any case, would it be accurate to say that based on the forensic evidence, something happened to that e-mail on April 29th of 2005, that was different than the explanation that Mr. Rote gave?
A. Yes.
MS. MARSHALL: Okay. Is it time for a

break?

ARBITRATOR CROW: No. I'm just trying to make sure I understand. If people want a break, we can break.

THE WITNESS: I wouldn't mind one.

MR. ROTE: I wouldn't mind one.

ARBITRATOR CROW: Why don't we take 15 minutes then.

(Break taken from * to *.)

ARBITRATOR CROW: Let's go back on the record.

MS. MARSHALL: Are you able to hear okay?

MR. ZWEIZIG: Yeah. I did want to is everybody here?

MS. MARSHALL: Everybody is here.

MR. ZWEIZIG: Whoever got this phone system picked out for me it is great this is a thousand times better than it was before.

MS. MARSHALL: Great.

ARBITRATOR CROW: Ms. Marshall, you're up.

Q. BY MS. MARSHALL: All right. Okay. I want to have move on to the other document that is actually discussed in Exhibit 68. So if you could keep that with you. But it is, it's the termination letter. And the termination letter

is Exhibit 13. Do you have that right there? 13 is the termination letter. Were you shown a copy of this letter and asked to perform some forensic examination?

A. Yes.

Q. Okay. And what were you asked to do relative to this letter? Here.

A. Let me start by saying originally with the stipulation order that I originally received, I wasn't asked anything specifically about this letter. I was only asked to go through the data that I was presented with, basically the hard drive, two hard drives and floppy disk, that they didn't really ask me anything specific. They just said look for anything related to Max's termination, you know. And so therefore, I didn't really have this letter necessarily compared to any other letter.

Q. Okay. But I've asked you to do some forensic examination with respect to this letter. And we refer to Exhibit 68, which you say is not in that book?

A. No.

Q. Okay. It will be in this book here. Exhibit 68

is the, as Mr. Williams' report that we were

just looking at. You might have even had it on your screen.

A. Okay.

Q. This is, Exhibit 68, page two, I guess, starts the discussion of what he refers to as Maxterm.doc?

A. Correct.

Q. Now, in 2008 when you came down to examine storage devices and whatnot, you were provided with a two and a half inch floppy disk; is that right?

A. Yes.

Q. Okay. And what were you told about that floppy disk?

A. I was told that it contained the copy of the Max termination letter.

Q. Okay. And who gave it to you?

A. Well, the floppy disk was originally given to me by Jeff Edelson, I think is what his name was. It was actually in the room. It was in Jeff Edelson's office along with the computers, two computers that were there, the laptop, Steve Rote's, I'm sorry, not Steve, Tim Rote's laptop

and the...

Q. Box?

A. Yeah.

Q. Okay. Let's just stick with the floppy disk.

Did you have an impression as to what the floppy disk was, what it represented?

A. The impression that I had, I'm sorry. The impression that I received was that it was simply a copy of, or it was a copy of the Max termination letter. Actually the impression that I was given is it was supposed to be the original Max termination letter, that it was created on that floppy disk when Tim Rote first created it.

Q. And was it marked in any way?

A. No, it was not.

Q. Did it have anything on it or in it to identify it as the original?

A. No.

Q. So how did you, well, first of all, how do you write protect a floppy disk?

A. Let's see here. Give me a moment. On a floppy disk, this is similar to the floppy disk that I

reviewed except for it was green. It was not marked at all. And on a floppy disk there is a tiny switch on the back, this one right here that goes up and down. And that is what sets it

to be either writable or read only where you can't write any data to it.

Q. When you received it, was the write protect switch on or off?

A. The write protect switch was off.

Q. Which means that it could be --

A. Written to.

Q. Written to?

A. Correct.

Q. And what did you do with the write protect switch?

A. I turned it to where it was read only so I could not write to it.

Q. Okay. And then did you create a bit by bit, a bit stream image of the floppy disk?

A. Yes, I did.

Q. Was there anyway that you could determine whether this floppy disk was the same floppy disk or the same image that, was it Mr. Williams originally imaged in June of 2005?

A. Yes. No. No. There was no way to tell.
Q. Why is that?
A. Mainly because there's nothing that marks it as original. It's similar to just taking a hard drive out without any sort of identification.

There's just no way to tell.
Q. Okay. Did, can you explain the concept of hash values.
A. Sure. So a hash value is basically an algorithm. They take every bit of byte that's on this data storage device. It could be huge. It could be like a hard drive. And they perform basically a mathematical equation against every bit or every set of bits on a data storage device. And the hash value at the end is, it becomes the, you know, the original or basically a finger print for whatever the hard drive, whatever that hard drive is. So the hash value in the cases when it comes to forensics is the way to tell if anything is changed on this disk or this drive or this original, you know, data storage device versus, you know, the next one you get or in order to tell that Steve's, when

he took the image, the hard drive matches the same image that I took when you performed my data, my forensic imaging.

Q. Did you have the hash values that were taken when he took his image of the floppy?

A. No, I did not.

Q. Okay. But you created, your imaging device

created hash values; is that correct?

A. Yes. That's correct.

Q. And did that tell you whether you got a complete copy of the floppy disk?

A. Yes.

Q. Okay. Was there anything on the disk other than the termination letter?

A. Yes.

Q. Or Max dot --

A. Maxterm.doc?

Q. Uh-huh. What else was on that?

A. There was images, deleted images.

Q. Images as in pictures?

A. As in pictures.

Q. Okay. So it was basically a used floppy disk?

A. Yes, it was.

Q. Okay. Do you have your report there so that you

can refer to it if you need to?
A. Mine, yes, I do.
Q. All right. So after you took a bit by bit image of the floppy disk, did you analyze the image to determine what metadata might help you in determining whether that document was written in October of 2003?
A. Repeat the question, please.

Q. Okay. Did you analyze or examine the image that you took to determine whether there was metadata that would help you figure out whether the document was, in truth, created October 2nd or October 1st, I guess it is, of 2003?
A. I mean, I took an image and had my own hash value. But I could not, just having your own hash value doesn't tell you that this is necessarily the original or not. It just tells you that whatever your hash value is, you can have that compared to the next person who takes an image of this exact floppy.
Q. Okay. Let's, I think I'm confusing the issue by referring to hash values. In Mr. Williams' report, which is Exhibit 68, he reports that he

found that the dates and times for the creation, create date, modification date and last access date, were October 1st, 2003, at 9:29 a.m.

A. Okay.

Q. For two of those. Okay. Did you also look for that kind of metadata in the floppy, on the floppy disk?

A. No.

Q. Okay. What did you look for?

A. I looked to see what data existed on the floppy

disk and verified that there was no corruption on the floppy disk, meaning that the same thing, when you take an image, as I explained to you previously, on the laptop drive, how it reports bad areas, right, the floppy disk does a similar thing. Anything you take does a similar thing. So I can tell whether or not this was, the floppy disk was corrupt in any way.

Q. Okay. Was the floppy disk corrupt in any way?

A. No, it wasn't.

Q. Okay. Did you review Mr. Williams' report with respect to the metadata on the termination document?

A. Yes.

Q. And do you have that in front of you?
A. I don't have his report in front of me, no.
Q. Okay. Well, we can get it for you. It's number 68. It's right here. It's right here. All right. There it is. Exhibit 68, page three.
A. Got it.
Q. All right. And at the top he says, the dates and times associated with the document file entry are as follows, create date, October 1st, 2003, at 9:29 a.m., modification date, October 1st, 2003, at 9:29 a.m.

Does that in and of itself, is that sufficient to you to verify that that document was, in truth, created on October 1st, 2003?
A. No.
Q. Why not?
A. The reason being is the same reason as before is to prove how easy it is to change your date and time on the computer, well in this case, simply plugging this in having the read only switch off is where I can write to the disk, we'll create the same dates, modified create date modified and last access as I set my date and time to on

my computer. So therefore just because it says so on the disk that those are the dates and times, without seeing the original computer that it was actually created on, I'm unable to prove, you know, to the fact that that is exactly when it was really created.

Q. Okay. Well, let's -- Did you look at the document within the forensic tool that you had?

A. Yes, I did.

Q. Okay. And did you find discrepancies between the document is in or was on the floppy and the document that was actually printed out?

A. Yes, I did.

Q. Okay. Can you explain to us or show us what those discrepancies are?

A. Do we have the printed out one anywhere?

Q. We do. It would be right below here, Exhibit 13.

A. Got it. Okay. I noticed, I'm just going to open it up. I noticed that there was differences in the address, for starters. And unfortunately I don't think I have... . It's tough to tell off of this exhibit without really showing the demonstration on the computer. But

there was a difference for the date for starters, this date, the printed out date was ten two instead of 10-1. And it has a full date of 2003 instead of just a two digit date which is '03. The next thing down, this is all off my memory, the NJ for New Jersey, you know, in the original one it was spelled out as New Jersey instead of the two letter abbreviation. And there were some various other names or words in here that were, you know, misspelled or not capitalized or correctly, et cetera, that were also different between the one that was on the floppy disk and the one that was printed out and told that this was what Max Zweizig had

received.

Q. Okay. So would it be fair to describe Maxterm.doc on the floppy as appearing to be a draft?

A. Yes.

Q. Okay. Which, if it were finalized, turned into Exhibit 13; is that right?

A. That's correct.

Q. Okay. Based on, just based on the evidence that

we've talked about so far, the evidence that you see in Mr. Williams' report, the metadata that shows create date on October 1st and a modification date of October 1st and a last access date of October 1st, and your review of the letter in the forensic file, okay, is there any way that one can conclude that that document was actually finalized on October 2nd, 2003?

A. The only way to conclude it is if you had the original computer in which the document was created on.

Q. Okay. Well, then let's talk about the original computer. How do you know there was an original computer?

A. I know that because of the metadata that was found on the floppy disk that was taken, the

floppy disk image versus the, versus the image that the laptop had. So as an example, I think it's in my report, I have exhibits on here; right? Do we have the exhibits from my report?

Q. They should be attached to the report.

A. They're not on mine. There's an exhibit that shows a user name, a author, I should say, an author, an author's initials and the company. I

don't know where we're going to find it.

Q. Does it look like that?

ARBITRATOR CROW: We do have --

THE WITNESS: Close.

Q. BY MS. MARSHALL: Can you work with that?

A. This is more of it, yes.

Q. Let's use this.

ARBITRATOR CROW: What are you looking at?

THE WITNESS: This is 185 --

MS. MARSHALL: Mark this as Exhibit 185.

But I believe it was originally part of his report.

ARBITRATOR CROW: Well, show me on the report where it is. What page of the report? I've got arbitration Exhibit 103 and I've got pages eight, nine, ten, 11 --

THE WITNESS: This is actually part of my

report as page two, at least one of them is on page two. I should say two of them.

MS. MARSHALL: We need to make sure that he's got all of Exhibit 103.

THE WITNESS: This actually isn't mine.

Okay.

ARBITRATOR CROW: Well, let's take a look at Exhibit 185. What is it?

THE WITNESS: I tell you what I brought my file with me and this file contains the image on there. So if you don't mind -- I can't. I don't have the right thing for it.

Q. BY MS. MARSHALL: Is this what you are looking for?

A. We are getting there now. Yes. Okay. So Exhibit 103.

Q. What page?

A. 12 and 13.

ARBITRATOR CROW: Pages 12 and 13?

THE WITNESS: Yeah. 12 and 13 of Exhibit 103.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: Okay. Now, is this data off of the floppy data, the floppy disk?

A. This data actually is off of the laptop. And

then before that, let's see if I have it on here. Yeah.

ARBITRATOR CROW: I am looking at Exhibit 103, pages 12 and 13. It doesn't mean anything to me without your testimony. What aim

looking at?

THE WITNESS: Okay. So 12 and 13, you're going to see in the bold, these are the settings on the computer. Let's say, let me go open this up for you on the screen. You'll see that I go into, oops. This isn't, not the right computer. Let me get to a different computer here.

Okay. If I go open up Microsoft Word. All right. And let's make sure I have this right. User information. Okay. So here you see that under my name I've got NorthWest Direct employee and under my initials I have NDE. Okay. Well that's a setting on the computer. In the operating system there's a, an area called the registry and that registry is a big database. And that database holds all the configuration, most the configuration for your computer, including your configuration of Microsoft Office. All right. So whenever you write a document such as that Maxterm.doc that was on

that floppy disk, this data gets written with it. This data is actually part of the metadata that's on that document on the floppy disk.

So what this is showing on 12 and 13, it's simply showing in a very technical, nonlayman's term way of what those equal. So the one that says name user initials and then you'll see, if I can find it, one second, okay. So on 12 and 13 in the actual box, the boxes that are right here, these are the actual values that you'll see. So under user initials where it says registry key property value and you'll see R, that's all that was here in this area was here was an R. And then down below you'll seem the user name. That's this one where it says name. In this case it says Rote T for I'm assuming Tim Rote. This is coming off of the laptop. And then the next one down below is a company, which is, I don't remember where that is, company is actually here, properties. Company, it simply says NWD. Well that's what the laptop has programmed into it.

Q. BY MS. MARSHALL: Was the floppy disk, was the Maxterm.doc created on Mr. Rote's laptop?

A. Not based on this information. And the reason

being is because while Mr. Rote's laptop said R, Rote T and NWD for the information, the metadata

on that, on any document he creates, it's going to have that embedded into it. The one that's on the floppy did not have that information there. Therefore saying that it was not created on that laptop.

Q. Can you tell whether -- Now, you understand Mr. Rote testified that the, that the document, the termination document was created on the floppy and only saved to the floppy. Now, the floppy doesn't run by itself.

A. Right.

Q. So can you tell whether that is accurate?

A. Yes.

Q. Okay. By, based solely on the metadata in the floppy?

A. Yes.

Q. Okay. And here I guess I'm referring to Exhibit 185.

A. Yes. So she handed this over to you?

ARBITRATOR CROW: Yeah. I've got 185.

Q. BY MS. MARSHALL: And did this come off of the floppy itself?

A. This did.

Q. And what does it tell you? Starting at the top line.

A. Okay. So what happens is when you create a Word document and you first save it, like as an example you'll see on the screen here, I have nothing written on this Word document. If I go to save this document, it's going to ask me to save it into my documents under the name of doc1.doc. That's what this first line means on Exhibit 185 page one. It was actually saved into and on a hard drive a C drive. The C drive colon typically means a hard drive somewhere. So it was saved originally as doc1.doc meaning it had nothing in it. Because watch on the screen again if I type anything into this document like Maxterm, okay, let's say I type that and then I go hit the save button, then it's going to try to name my document after the first thing that I have written into it. So based on this information that's in Exhibit 185, it was first saved with nothing in it. Then what happens --

Q. BY MS. MARSHALL: Now, where was it saved?

A. It was saved on a C drive, or a hard drive underneath the user name of owner.

Q. Okay. Now, let's stop there. How do you know that it was saved --
A. Sorry.
Q. You're kind of fast for me anyway.
A. I am.
Q. How do you know it was initially saved to a hard drive of a computer?
A. Well, it's an assumption, but based on the typical operation of computers and of the Windows operating system, the C drive, C colon backslash is almost always the 1 hard drive on a computer. Right. Take a look at this computer here, okay, the C drive is my hard drive.
Q. Okay. And what is typically the floppy drive?
A. Typically the floppy drive would be an A drive.
Q. Okay. So let's go back to the C drive now. Do we know what hard drive it was that this document was created and saved to?
A. No. All we know is that this hard drive, that inn that specific location on the hard drive, does not match the laptop.
Q. So it wasn't the laptop, but it was a computer.
A. Yes.
Q. Now, have you read Mr. Rote's testimony about, that he created this document on a computer at

the NDT call center in Eugene?
A. Yes, I have.
Q. But did not save it to the computer. He saved it to the laptop. So are you saying that that's not exactly accurate? It was saved to a computer?
A. That is exactly what I'm saying.
Q. Okay. Now, when it was saved to that computer, would the computer, would the hard drive, the operating system on that hard drive create additional metadata that's not on the floppy?
A. Rephrase, please.
Q. Okay. Well, let's start with the save, the initial saving, the doc1.doc.
A. Yes.
Q. Did doc1.doc have metadata associated with it on the hard drive of that computer?
A. Absolutely.
Q. And would that metadata tell you the date and time that the document was created?
A. Yes, it would have.
Q. If you had the computer?
A. If I had the original computer.
Q. Now, when you work on a document on, even --

ARBITRATOR CROW: Unless it was overwritten.

THE WITNESS: Unless it was overwritten.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: When you work on a computer using a floppy, does the operating system, the Windows system, capture or save that document in any other way for you?

A. Yes, it does.

Q. How is that?

A. It has what's called an auto recovery. Again, if you don't mind me demonstrating.

ARBITRATOR CROW: No. No.

THE WITNESS: If you go again into the options -- they changed it on this one. If you go into the options, you'll notice that it has an auto recover in here. And by default it's set to three minutes, I think if I go, let me exactly show you.

Q. BY MS. MARSHALL: So you're saying every three minutes the computer automatically saves the Document 4?

A. That's correct.

Q. And if you do a forensic examination of that computer, are you able to find, assuming it

hasn't been overwritten, are you able to find metadata associated with that auto recovery

file?

A. Yes.

Q. Okay. Are there, and that would be date and time as well?

A. Yes.

Q. Now, are there other files --

A. If you don't mind me interrupting you.

Q. Go ahead.

A. Basically this doc1 and this auto recovery save of doc1 will basically be the same exact file with the same metadata except if Tim, as an example, were writing in this document and three minutes later it saves, then that information, whatever he wrote, will be in there along with all the metadata.

Q. Okay. Are there other files that the original -- Can we call it the originating computer now, that the originating computer, are there other files that it will save your document to?

A. Yes.

Q. And what are those called?
A. Those are called temporary files.
Q. So this is a third file that the document is created and saved to automatically; is that

right?
A. That is correct.
Q. All right. On the originating computer. Do the temporary files have metadata associated with them that include date and time?
A. Yes, they do.
Q. And if you had the original computer, the originating computer and it was not overwritten, would you be able to identify the date and time that that document was created?
A. I'd be able to identify the date and time that document was created as well as look at log files to make sure the date and time wasn't manipulated on the original computer.
Q. Okay. Were you ever provided the original, the originating computer to examine?
A. No, I wasn't.
Q. Did you make people aware of the fact that there was a computer out there that had metadata on it you wanted to look at?

A. I did through my report.
Q. Okay. Well, you have the report. You also prepared and submitted a couple of declarations in which you describe that.
A. That's correct.

Q. Is that correct?
A. Yes.
Q. Were you ever permitted to examine the originating computer?
A. No, I was not.
Q. Do you know whether Mr. Williams or Mr. Cox ever examined the originating computer?
A. I do not.
Q. Without examining the originating computer, can you say with any degree of scientific certainty whether the metadata on the floppy is accurate?
A. No, I can't.
Q. All right. Let's talk a little bit more about Exhibit 185 because there's three lines there that I need to understand. And I think probably Mr. Crow would appreciate an explanation.
You've talked about the document was manually saved by Mr. Rote or whoever the

operator was once.

A. Correct.

Q. And you've talked about the temporary files and you have talked about auto recovery. Is there metadata here that tells you about the document being saved to a floppy?

A. Yes, it does.

Q. Tell us what that is.

A. So with 185, the way that the metadata works within a document, even without originally necessarily being saved, but in this case it was saved as doc1.doc. After that within three minutes it was saved, it was auto recovery saved that same document as the auto recovery save of doc1.ASD. Even though it has a different extension, the ASD, it is still a document. So it still has the same metadata embedded within it. And then finally it was saved to an A drive, typically a floppy disk, as Maxterm.doc. So that tells me that there's three locations that this document existed in.

Now, if you have a look at my screen, I did the same exact order. I saved it as doc1.doc. I will waited until it did an auto save, auto

recovery and then I saved it to a floppy disk. And if you look at the disk now you'll see this exclamation mark WRD3744.temp. That is the temp file that I was referring to that is always created wherever you save this document. You'll notice it's the same exact size at the Maxterm.doc. So from a forensics perspective, if the floppy disk that we were given, the green

floppy disk was the original, the original one where he said, where Tim Rote stated he only saved it to that floppy disk we would be able to see the temp file from that creation of that document. But we were unable to.

Q. So are you telling us that you were not given even the original floppy disk on which the document was created?

A. That's correct.

Q. And you can tell that because it does not have the metadata in it that you would expect?

A. Because it does not have metadata that matches the laptop and does not have a temporary file. We cannot see the deleted temporary file even though we can see all the deleted pictures that

were on that floppy disk. So it tells me that that was not the original floppy Maxterm.doc was create on.

Q. Okay. Now, let's just, before we leave the originating computer, in your judgment would the concept of litigation hold have applied to the originating computer?

A. Yes.

Q. And so it should have been preserved or at least the hard drive of that computer preserved or

imaged early on, and if it had been, what would you be able to do with it?

A. A few things. I'd be able to match the metadata between the document that was written, that goes with the owner, the user initials and the company. I'd be able to match the metadata and actually find the metadata and the document piece, at least pieces of the document that still existed according to where this says it was saved. I'd be able to term determine if or when that document was originally created, how many times or when it was last accessed, as well as looking at the log files and such in order to determine if the date was ever manipulated. So

quite a few things if I had that original computer in front of me.

Q. Okay. And by, by not providing that commuter to either you or either of the other two experts for examination so that you could even, even if you could review their images, you don't have any images, did that put Mr. Zweizig at a disadvantage?

A. Absolutely. I mean, it means that he could not get any of the original information to, again, disprove or prove his case.

Q. Okay. Let's go back to the floppy now. In the Exhibit 68, which is I think still over here, Mr. Williams' report where he has the metadata create date and that's October 2nd, 2003, at 9:29 a.m. excuse me. October 1st at 9:29 p.m., or a.m. modification date October 1st, 2003, at 9:29 a.m. just as I call the eyeball test, does that suggest to you that this file was simply copied from somewhere else?

A. Yes, it does. As Mr. Williams explained earlier during his redirect, just copying files over to a location will, will affect the last, sometimes

the, usually what was getting at is it will affect the file created date on any file system that is there. When it comes to a floppy disk, it has a different type of file system than what he was referring to earlier, and, therefore, if you copy a file over to it, the last, the file created data long with the file modified date, the modification date will be exactly the same. So therefore, based on the image that was, that we took that Steve Williams took as well as myself of that, supposedly original green floppy, it wasn't the original, it was a copy of the document onto that floppy disk.

Q. Okay. Now, you've read Mr. Rote's testimony where he said that he created this document on the floppy, saved it only to the floppy and carried the floppy home with him, and that is the floppy that he produced, can you say with any degree, with any degree of scientific certainty that that was not how that document was created?

A. Yes, exactly how I just explained. It does not contain temporary files. The dates are completely the same on the created and the

modified which shows that it was copied over to the disk and not created on it.

Q. So if the, if the document was not created -- Well maybe I should ask you. Was the document, do you have any idea whether the document was created on Mr. Rote's laptop?

A. No. I mean --

Q. I asked a bad question. Yeah?

A. Yeah. Rephrase that, please.

Q. Was it created on Mr. Rote's laptop?

A. No.

Q. And how do you know that?

A. Because the metadata does not match the laptop, both the metadata does not match the laptop for

the user name, the user initials and the company and the metadata does not match from Exhibit 185 of the location. This documents, the settings backslash owner -- I'm slowing down a little bit for you -- the documents and settings, backslash owner is the sign of the win domes operating system Microsoft Windows XP home, not professional. So that tells me that whatever computer was utilizing this software had the XP

home on it instead of XP professional. The laptop that Mr. Rote provided was XP professional. So that's another indication that this was not created on his laptop.

Q. Okay. Now, there's another really simple one. The laptop didn't have a slot for a two and a half inch floppy, did it?

A. From my pictures and my memory, that's correct.

Q. Okay. So if the floppy disk that you were provided was simply, had simply been copied from somewhere else, okay, how was that copy created? Can you explain how the copy was created?

A. If it was from somewhere else, meaning not on his laptop, it means that the drive, the computer that he utilized had a floppy disk or he was able to connect one up to it in order to

copy it from the hard drive where it was located over to the floppy disk.

Q. Okay. So based on the information we have here, you didn't see the originating computer. You've never seen the original floppy and do we know what computer was used to create the copy of the, that went onto this floppy?

A. No, we don't.

Q. And that computer obviously would have metadata in it as well?
A. Yes, it would.
Q. Okay. All right. So Mr. Rote testified, you recall reading Mr. Rote testified that he took the floppy home with him with Maxterm.doc on it and either that evening or the next day opened it, changed date and printed it. Okay. Can you tell from the information, the metadata that you were provided, that you got from the floppy, whether that's accurate?
A. No. No, you can't.
Q. And why is that?
A. Because if even printing it as I mentioned earlier, the metadata in the document also saves when it was last printed.
Q. Okay. So if we had the original floppy that he

says he carried home, we would be able to see metadata that would show when it was opened and printed?
A. No.
Q. Okay. Where do we have to look for the open and printed?

A. We have to look on his home PC.
Q. So that is now a third computer that may have metadata on it that would show the date and time that this document was created?
A. Yes.
Q. Did you, were you ever able to examine that computer?
A. No.
Q. So if we can call that the modifying computer or the second computer, what can metadata would have, would that date, computer have on its hard drive?
A. Similar to the originating computer, it would have information about when it was accessed, the date and times of when it was accessed, how many times it was accessed, when it was printed and it would also, it would also contain an auto recovery, depending on how long the document was open for on that computer.

Q. Okay. Particularly the computer that was used to open the floppy and revise it and print it out, okay, the failure to provide that computer for examination, was that a particularly prejudicial thing as far as Mr. Zweizig is

concerned?
A. My opinion, my opinion is that that was almost as valuable as the original computer that it was created on. Not as valuable only because the original computer should show the original date or have, give someone like me the ability to check the original date when it was actually created versus what we've been told and what was on the floppy disk. That may or may not exist on the secondary computer.
Q. Okay. But the secondary computer would tell you when it was printed; correct?
A. Yes. Yes, that's correct.
Q. Now, I have to ask you not to speculate but I am going to speculate and give you a hypothetical. Okay. Let's say that Mr. Rote, and fed a peek or whatever on October 1st thought about firing Mr. Zweizig, sat down and drafted the letter and then thought better of it and didn't, didn't send it. Okay. The metadata that we see in

Mr. William's report that you have described would all be there, it was created on October 1st?

A. That's correct.
Q. Okay. But you can't tell whether it was printed on October 2nd without the second computer, can you?
A. That's correct as well.
Q. Is it possible that even though it was created on October 1st, it could have been printed on October 30th after maybe other incidents have happened?
A. Without having the computers around that it was printed on, there's no way to tell. So it's possible, absolutely possible.
Q. So am I accurate in concluding that the metadata in Mr. Williams' report describes a draft and nothing more?
A. Possibly.
Q. Okay. Well, I asked Mr. Williams whether it was possible, whether three scenarios are possible, one is that one could reset the clock and type the letter up any time you want and it would show that metadata. If you told the computer it was October 1st, that's what the computer would

think. The second is that you could draft the letter on October 1st, think better of it,

change your mind, whatever, and then after incidents later in the month, decide, by golly, I am going to fire him. So then you finalize the document and print it. That's possible given the metadata that we have, isn't it?

A. Yes.

Q. And then of course the third possibility is that it could have been printed the next day but we can't test that because we don't have the computers; right?

A. That's correct.

Q. Okay. You mentioned earlier, and I'm just going to go into this for just a few minutes and then we can take a break for lunch. But you mentioned earlier that, where you asked to look for evidence of the exit time e-mail on the computer that Mr. Zweizig used, the Sony Vaio computer.

A. That's correct.

Q. Okay. Well, let's go back to when you received that computer. When was it that you examined that computer?

A. December 12, 2008.

Q. Okay. Same time that you got the floppy and examined Mr. Rote's laptop?
A. That's correct.
Q. And was the 60-gigabyte installed in the computer?
A. Yes, it was.
Q. So you were able to match it up and tell that that actually ran on that computer; right?
A. Yes. Yes.
Q. And did you make a forensic image of the 60-gigabyte hard drive?
A. Yes, I did.
Q. And the same way that Mr. Williams described that he had made a forensic image?
A. Correct.
Q. And did you examine that, well let me ask you, what were the issues that you were asked to examine that 60-gigabyte hard drive for?
A. I was asked to actually examine the 60-gigabyte hard drive, the laptop drive as well as 120 gigabyte hard drive for any, any relevant documents dealing with Max's termination in the year 2003. That's the first thing I was asked by the stipulation order.
The second thing I was asked was to review

the same data storage devices for any sign of basically nonbusiness related activity such as pornography or games or, you know, internet activity, that type of --

ARBITRATOR CROW: On which computers.

THE WITNESS: This is all of them, this was from the stipulation order. It was not specific about which computers. It was more or less saying that all of the data storage devices that I was provided by Edelson at the time and Tim Rote, I was supposed to go through and review all of the data storage devices for this information. And finally I was supposed to check to see if any, any deletion or programs on there were deleted, especially using any sort of deletion tools.

Q. BY MS. MARSHALL: Okay. So let's just focus on the e-mails. Did you examine the 60-gigabyte hard drive in December or January of 2000 -- I guess it was December of 2008, did you examine it for evidence of e-mails, specifically the exit time e-mail?

A. No. I, like I said, I was, I specifically, well not specifically. I generally was looking for anything having to do with Max's termination in

the year of 2003. I was not specifically looking for e-mails and I was not specifically looking for the exit time e-mail.

Q. Okay. So you're looking generally for anything having to do with the termination. Did you find anything?

A. Yes, I did.

Q. What did you find?

A. I found the exit time e-mail as an example. I'm sorry. Not on the 60-gig. I found nothing.

ARBITRATOR CROW: Nothing on the 60.

THE WITNESS: I found absolutely nothing on the 60-gig Drive. Excuse me.

Q. BY MS. MARSHALL: Okay. You know that Mr. Cox did an examination of the 60 either in 2009 or 2010. And also found no e-mail traffic on the 60.

A. I am aware.

Q. Did you, did you review Mr. Williams' report to see whether he found any evidence of e-mails on the 60?

A. Yes, I did.

Q. This is back in 2005. And he found a series of e-mails, did he not?

A. That is correct.

Q. Okay. And I want to draw your attention to one of them, in particular. This is Exhibit 71. You will find it over here. 71. Okay. Page eight.

ARBITRATOR CROW: Page eight.

Q. BY MS. MARSHALL: Yes. I'm sorry. I should have let you --

A. No problem. Okay.

Q. Now page eight number five. Now there's been some testimony about, that these e-mails were just parts of e-mails that were sent to somebody else. Number five here, in Mr. Williams' report, is printed off of the Sony Vaio in 2005. Well, tell us what that file, that line of file information tells us?

A. That path?

Q. Yes. File path?

A. That file path indicates that it's an Outlook storage file for all e-mail coming into Outlook and that it belongs to the account Jay Cioffi, which I believe was owned by Joe Cioffi from NorthWest Direct.

Q. Okay. And it's an Outlook PST file?

A. That's correct and it is not deleted.
Q. And it's not in deleted space?

A. No.
Q. Okay. And it says original message from Irene a somebody, *Ranoff, to Brent *Cowiak and Max@NWtelemarketing.com.
A. Correct.
Q. Do you see that? Now, would that indicate to you that at some point in time prior to at least 2005, that computer had been used to receive that original message?
A. Yes.
Q. Okay. Did you see that message when you went looking for e-mails in 2008?
A. No.
Q. Do you have any idea why?
A. Two reasons. One, it did not match the search terms that I am put in for termination for Max termination, and second, it could have been deleted years later and I would not have been able to find it.
Q. But Mr. Cox couldn't find it either and he was, he did testify that he was looking for that,

that e-mail address?

A. That's correct.

Q. Okay. So, in your judgment what would explain why Mr. Williams would find it in 2005 and

Mr. Cox would not find it in 2009 or 2010?

A. The latter of my previous explanation. It means it was deleted and overwritten by the time that Mr. Cox was doing his search. And I should add onto that, just because he didn't find it could mean that just the very top portion with Max's e-mail part was deleted, not necessarily the entire e-mail. But he wouldn't have hit on the rest of this e-mail without, because he was searching for Max only.

Q. I'm not sure I follow you.

A. Okay. So in forensics we use keywords to do our searches across the entire data storage device. Right. And in Mr. Cox's case my assumption is that he searched for Max@NWtelemarketing or he just searched for Max, just as an example. Well, if, if part of this file got wiped out like that original message and down four lines, that got wiped out but the rest this have still existed, he would not have found it because

nothing else in this message matches Max or Max@NWtelemarketing.com. So it's possible that this still exists on the hard drive, just not the portion that is on the very top.

Q. Okay. So in your judgment would you say that

the conclusion that the 60-gigabyte hard drive was never, most certainly never used to receive e-mails or reach?

A. I don't agree with that. So it was used, definitely used for e-mail at one point in time.

MS. MARSHALL: All right. If it would be okay, it's straight up 12:00. And.

ARBITRATOR CROW: That's fine for a break.

MS. MARSHALL: It would be.

ARBITRATOR CROW: If you would like to do that.

MS. MARSHALL: I would.

ARBITRATOR CROW: All right. We'll go off the record.

(Break taken from * to *.)

ARBITRATOR CROW: All right. Go ahead.

Q. BY MS. MARSHALL: I want to, I may have confused an issue this morning in the way I asked a

question. And so I just want to make sure that Mr. McAnn has an opportunity to clarify. And it's just a very simple question relating to the exit time e-mail. When you move an e-mail from one folder to another, does it change the last modified date?

A. And the answer is no, it does not.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: And you're certain of that?

A. I am absolutely certain of that.

Q. All right. Let's finish up talking about the 60-gigabyte hard drive that you examined. I believe you said that you were instructed, first of all, to look for anything related to Mr. Zweizig's termination.

A. Yes.

Q. And the other issue that you were asked to look for was extra job kinds of activities like porn.

A. That's correct.

Q. All right. Did you examine the 60-gigabyte hard drive, the image of the 60-gigabyte hard drive for porn?

A. Yes, I did.

Q. Okay. And did you find any?

A. No, I did not.
Q. Did you find an image or any images on the 60-gigabyte hard drive that could be considered to be porn?
A. No, I did not find any images at all. The only thing that I found similar to Mr. Cox, is, and maybe even Steve Williams, if I remember right, is file names that represent or could be

pornography. However, all of the file names and --
Q. Okay. Before you go any further, I'm still talking about the 60-gigabyte not the 120-gigabyte?
A. My fault. Sorry.
Q. It might have been mine. Just sticking with the 60-gigabyte hard drive for the moment, did you search it for anything that might be porn?
A. Yes.
Q. Okay. And what did you find?
A. I didn't find anything that related to porn at all in the 60-gigabyte hard drive.
Q. Okay. Now, do you have experience that would permit you to examine with some authority

looking for porn?

A. Yes. During my time working for different corporations, that goes for AT&T wireless for nine years as well as *PACR for two years, a lot of their cases are considered policy violations. So most of the cases that I do on a corporate level are pornography cases. That's hundred, I've done at least 100 pornography cases.

Q. Okay. And how do you go about examining an image to look for porn?

A. Typically what you do is you start off doing what they call a gallery mode or a gallery view to where you are viewing every picture that exists on that data storage device. And you go through it page at a time, no matter how many images there are in looking for specific, you know, flesh tones or specific images.

Q. Okay. And in this case did you do that with the 60-gigabyte?

A. Yes, I did.

Q. And what did you find?

A. I did not find any pornography.

Q. Okay. Did you find any images that could be considered pornographic?

A. No, I did not. Not on the 60-gigabyte hard drive.
Q. Okay. I just want to make --
A. I'm sorry.
Q. Make sure we are you can talking about the same hard drive I am thinking about and the same images I am thinking about.
A. I'm sorry. Must be the lunch I did, I found three, three images that could be considered pornographic.
ARBITRATOR CROW: On the 60-gigabyte.

THE WITNESS: On the 60-gigabyte hard drive.
Q. BY MS. MARSHALL: Okay. And without getting into too much detail can you tell us what those three are?
A. There were two images of male genitalia and one image of a woman's breast.
Q. And in terms of --
ARBITRATOR CROW: That's on the image, not on a hard drive? Am I correct?
THE WITNESS: No. Those are images that are on the 60-gigabyte hard drive.
ARBITRATOR CROW: Oh. I understood you to

say earlier that you found no pornographic reference on the 60-gigabyte hard drive.

THE WITNESS: That's my fault because I wasn't paying attention.

ARBITRATOR CROW: All right. So I didn't hear you wrong. You did say that.

THE WITNESS: That's correct. I spoke wrong.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: I want him to stay for a moment with the 60. And I want him to talk about the images he found on the 60-gigabyte hard drive. And with respect to those three

images, two of male genitalia, one of female breasts, what can you tell us that's relevant to this case?

A. I can tell you that one of the pictures occurred, well, had a date and time stamp of September, I believe, 2003. Yep. September 30th, 2003. The other two images did not, and unfortunately without my exhibits I can't tell you when they were, but they, the other two, one of the male genitalia and one of the woman's breast actually belonged to the

account named Jay Cioffi. So Joe Cioffi's account.

Q. Okay. And speaking just of the image that had at least a date of September of 2003, what did you do to investigate that image?

A. I tried to review all activity around that image, whether, so that means who accessed it, where did it come from.

ARBITRATOR CROW: On the 9-30?

THE WITNESS: On the 9-30 image, correct. The 9-30 image was underneath the profile NWT employee. So it's somewhat generic. And what I found is that that specific picture was accessed twice by the Jay Cioffi account. Again, and

that's actually on page, that's on Exhibit 103, page 11, where the Jay Cioffi account accessed that image once in December of '04 and again in July of '08.

ARBITRATOR CROW: But as I understand it, the 60-gigabyte hard drive was in the possession of Mr. Zweizig until sometime in October 2003. Is that not correct.

THE WITNESS: November, I believe of 2003.

ARBITRATOR CROW: November of 2003. So the access to the one picture on 9-30-03 would have been at a time when it was in Mr. Zweizig's possession?

THE WITNESS: It wasn't actually accessed on 9-30-03. That's simply the date and time like the creation date and time stamp as well as the last written date and time stamp. There's a, there's a difference between looking for activity and activity showing that somebody actually went to that picture and touched it versus a date that says it was touched by something. An example, if you look again on page 11 of example, of Exhibit 103, you'll see last access date. And those could be caused by anything. They could be your anti virus

programming touching them to make sure they're not viral.

ARBITRATOR CROW: Okay. I'm not sure but what we're off on a side bit of testimony here, I don't recall having seen or heard any testimony that would suggest NorthWest Direct tell services had a policy which would prevent an employee from accessing whatever he or she

wanted to during particularly during nonworking hours. Has there been any such testimony?

MS. MARSHALL: Not only has there not been any such testimony, but there are policies in the, that are in evidence that specifically allow employees to do personal things, they don't specifically allow viewing images, but --

ARBITRATOR CROW: But they don't prohibit it. That was my recollection as well.

MS. MARSHALL: That's right.

ARBITRATOR CROW: All right.

Q. BY MS. MARSHALL: So you were asked to find those and you did; is that correct?

A. That's correct.

Q. Okay. I think the third issue that you were asked to explore is whether there was any evidence that any data was intentionally deleted

or destroyed, in other words, any use of mal ware or anything of that nature.

A. Correct.

Q. Do you have experience that would allow you to look for that?

A. Again, I specialize in incident response, which

comes to computer compromises. So I have a lot of experience when it comes to utilizing applications to delete data, hide data, et cetera.

Q. Okay. And did you find any evidence that Mr. Zweizig had deleted or hid data?

A. I did not find any evidence that he deleted or hid any data. I did find an application that was installed on the computer that was part of their standard business practice called PGP, which stand for pretty good privacy, which has the ability to write or wipe, I'm sorry, wipe data. However, it, it just as I said in my report, it leaves a very specific signature and that signature did not exist at least in the image that I was able to examine.

ARBITRATOR CROW: The software was there but it doesn't show that it had been used, is that what you're saying.

THE WITNESS: By looking at the deleted data it doesn't look like anything was wiped using that software.

Q. BY MS. MARSHALL: Okay. Now do you know what the software was there for?

A. The software would be there to encrypted data such as private data for either their company or other companies in order to protect it from being compromised.
Q. When it was sent from client to --
A. Exactly.
Q. -- et cetera, back and forth. Okay. What would be the signature that you would see if it were used to actually wipe something off of the 60-gigabyte?
A. It would do a, it would do 255 characters because that's the maximum length you can have for a file name of like all A's or all B's or all something like that. And it would do that whether it's a file or a folder.
Q. And you didn't find any of those?
A. I did not find that.
Q. All right. Did you find any evidence that any Fox Pro files had been deleted?
A. I did find Fox Pro files on there that were

deleted but they were deleted after the date, after the 2003 date that Max Zweizig was, supposedly had that computer in his possession.

ARBITRATOR CROW: Wait just a moment.

Q. BY MS. MARSHALL: Okay. Let's move on to --

ARBITRATOR CROW: Wait a minute.

(Record read.*

ARBITRATOR CROW: Could you do you mean after it was no longer in his possession?

THE WITNESS: After 11-13-2003.

ARBITRATOR CROW: Okay. That was my confusion. Go ahead.

Q. BY MS. MARSHALL: Let's go on to the 120-gigabyte hard drive. I want to talk about your examination of the hard drive. When you went to Mr. Rote's attorney's office in December of 2008, were you provided the hard drive at that time?

A. No. Well --

Q. What were you given?

A. I was provided a box that was meant for a CD rom and was told that the 120-gigabyte hard drive was in that CD rom box.

Q. What was in the CD rom?

A. A CD rom.

Q. Is it hard to tell the difference between a CD rom drive and a hard drive?

A. No, it's not.
Q. So what did you do?
A. I told, actually Mr. Edelson was not there. So I told Mr. Edelson's assistant that it did not contain the 120-gigabyte hard drive --
ARBITRATOR CROW: I can hear you.
THE WITNESS: I'm sorry.
ARBITRATOR CROW: Don't worry. I'm not a jury.
THE WITNESS: So I explained that they, that it did not con taint 120-gigabyte hard drive. So they contacted Edelson, who contacted somebody else and I believe they may have contacted Mr. Rote at that time and said that they must have replaced or misplaced it and that I would have to come back at a later time.
Q. Okay. So then did you make another trip back here from Seattle to, at another, at a later date?
A. I did. So that was in December of '08 that I came back and sorry I was moving around. I am just going to go pull up my invoice so I can remember the date in February but it's probably

not as important. I came back in February because they said they had found the hard drive and that I was going to be able to come back and take an image of the 120-gigabyte hard drive.

ARBITRATOR CROW: February 2008.

THE WITNESS: February 2009. So when I got there they said there was some confusion, that they didn't have anything scheduled for me to be there. They sent me back home to Seattle without taking the image or even seeing that it was there or not.

Q. BY MS. MARSHALL: Okay. So did you go back a third time?

A. I did. I came back on March 20th, 2009.

Q. And at that time did they give you access to the hard drive?

A. Well, again I was under the assumption that they had found the hard drive. And in this case Tim Rote was there and the, they presented me or provided me a external drive that contained an image of the supposed hard drive on there. So I contacted at the time James Dow, who was the attorney for Max Zweizig, and they just said, well they couldn't find the hard drive, the original hard drive, but Steve Williams was able

to find an image of the hard drive and provide a copy of it. So that is what was contained supposedly on that external drive that they provided me.

Q. Okay. So what did you do with the external drive that they provided to you?

A. I basically took an image of an image, if that makes any sense.

ARBITRATOR CROW: I understand.

Q. BY MS. MARSHALL: Okay. Now, was there anything else on that hard drive?

A. There was other pictures, other documents, et cetera, all deleted. So in other words, it wasn't a clean target drive like we, in our field our practice to do. It could have been old case documents, it could have been his own documents. I'm not sure. I didn't go into that much detail.

ARBITRATOR CROW: Did you ever examine the 120 gigabyte hard drive.

THE WITNESS: Yes, I did.

Q. BY MS. MARSHALL: Well, the question is did you ever examine the hard drive?

A. No.

ARBITRATOR CROW: Okay. You just had an

image of an image.

THE WITNESS: (No audible response.)

ARBITRATOR CROW: All right. Thank you.

THE WITNESS: Sorry. Yes.

Q. BY MS. MARSHALL: So what does this, as a forensic examiner, what does this tell you about the litigation hold with respect to the 120-gigabyte hard drive?

A. It tells me it wasn't handled properly, that the chain of custody was corrupt. Therefore, they had, they seemed to have lost the drive.

Q. I just want to ask you one question with respect to your search of that drive, of that image, of the image of the image. Did you find in your search any evidence that Max Zweizig was participating in any kind of a pedophilia website?

A. No.

Q. Did you find any evidence that he was, that he had downloaded a video of pedophilia activity?

A. No.

Q. Okay?

MS. MARSHALL: I think that's all the questions I have at this time.

ARBITRATOR CROW: Tim, before you ask any

questions, let me understand --

MR. ROTE: Sure.

ARBITRATOR CROW: -- some things here. You did discuss briefly a question of deletion of files on the 60-gigabyte hard drive and you found no deletions that took place until after November 13, 2003. Is that correct?

THE WITNESS: That's correct.

ARBITRATOR CROW: Did you look for deletions with respect to the 120 gigabyte hard drive image that you had?

THE WITNESS: Yes, I did.

ARBITRATOR CROW: And did you find evidence of deletions on that image?

THE WITNESS: I found over 1900 different Fox Pro files that had been deleted.

ARBITRATOR CROW: And could you tell when they were deleted? 120 of them deleted, did you say?

THE WITNESS: No. 1900. Let me refer to my, my report.

MS. MARSHALL: I want to make sure that we're talking about the same drive, too.

ARBITRATOR CROW: We're talking about the 120-gigabyte image of an image; is that correct?

That's what you had to examine?

THE WITNESS: Yes.

ARBITRATOR CROW: And you found 1900 deletions. Can you give me an idea of what those deletions were and when they were made?

THE WITNESS: I can tell you only based on my report that they were Fox Pro type files. However, I did not, I did not document the dates or date ranges of those files that were deleted on the 120-gigabyte hard drive.

ARBITRATOR CROW: Let me see if I understand a little bit of your testimony.

THE WITNESS: Oh.

ARBITRATOR CROW: Go ahead.

THE WITNESS: Actually now that I think about it, I did document the files that were on the 120-gigabyte hard drive. That was one of my exhibits that I turned over to Edelson. And I don't know if it's turned into an exhibit here or not. It was exhibit, for me, I turned it over and it was Exhibit 10.

ARBITRATOR CROW: To your report?

THE WITNESS: To my report. To my original report. Exhibit 10 was the complete file listing of the 120-gigabyte hard drive.

MS. MARSHALL: We need make sure that you have a complete copy of that exhibit.

ARBITRATOR CROW: I think I do. That exhibit is number.

THE WITNESS: 103.

ARBITRATOR CROW: -- 103. Yeah.

THE WITNESS: But they didn't include them, I don't believe.

ARBITRATOR CROW: I think I've got, hold on. Let me make sure that I have it. Would it be page ten of your report, which has, that has a picture of the male genitalia, page ten.

THE WITNESS: Right. I do not see --

ARBITRATOR CROW: So I don't have anything from you which shows what deletions, if any, were made on the 120 gigabyte hard drive; is that correct?

THE WITNESS: It appears so, yes.

ARBITRATOR CROW: All right.

MS. MARSHALL: If it's okay, we can, we can

make sure that that exhibit is complete. It doesn't appear that it is at the moment.

ARBITRATOR CROW: Well, that would require some testimony as well as some cross-examination and the cross-examination would be impossible.

MS. MARSHALL: Okay.

ARBITRATOR CROW: Let me understand a bit. As I understand it you're unable to determine the date and time of the creation or the sending of the e-mail notifying Mr. Zweizig that he was terminated?

THE WITNESS: No. I was able to determine date and time that was on the e-mail. I was unable to determine if that date and time was the true and accurate time.

ARBITRATOR CROW: That's right. And I understand that the spoliation argument testimony and the lack of the litigation hold that might interfere with your ability to recreate that information. As I understand it, your testimony is the same with respect to the termination letter.

THE WITNESS: Yes, sir.

ARBITRATOR CROW: All right. Let me say while I'm focused on this then for both of you, I would like to have from each of you some law about presumptions, whether I should presume that there was spoliation because of the lack of litigation hold, whether I should presume that e-mails and letters were sent on the date

identified on those documents. As I recall before we had e-mail, there was a presumption that a letter was sent and received on or about the date it was dated. I don't know that that presumption holds true with respect to e-mail or not. But I need some help from both of you on that issue.

I also would like to have from you, Mr. Rote, a reference to anything that is in the record about advice to you of the need for a litigation hold. You now understand what a litigation hold is, I assume.

MR. ROTE: Yes, I do.

ARBITRATOR CROW: If there's anything in the record that relates to any advice to you about that issue, I would like to have you point that out to me.

MR. ROTE: Okay.

ARBITRATOR CROW: Okay. Cross-examination.

Q. BY MR. ROTE: Okay. I have, with respect to your arbitration Exhibit 103, only attached exhibits one through eight. I don't have nine and ten. But let's go and talk about some of the issues. Your conclusions with respect to the 120-gig hard drive was that it was

reformatted on November 12th, 2003.

A. That is correct. Which Exhibit No. Are you looking at?

Q. I was unable to find exhibits beyond eight in my records.

ARBITRATOR CROW: On Exhibit 103 you are talking about.

MR. ROTE: On Exhibit 103. I had separate records but I had only exhibits one through eight. Only a few exhibits are attached as part of this report. So we're still kind of back to some of the exhibits in your original report never made it into the record.

THE WITNESS: Okay.

Q. BY MR. ROTE: But let's go on with respect to

the question which was that you concluded that the 120-gigabyte hard drive had been reformatted on November 12, 2003?

A. That's correct.

Q. And that was during the time that Max Zweizig had that computer?

A. The date and time was supposedly during the time that Max Zweizig had that computer, yes.

Q. Now, many of the files that you also identified that were deleted I presume were zip files, had

NWD identifications, do you recall?

A. No. The files that I found, the 1900, is that what you're referring to?

Q. Yes, I am.

A. Those 1900 were simply based on extensions for Fox Pro files.

Q. So they were all Fox Pro files?

A. Yeah. FXT's, anything like that.

Q. So in addition to those 1900, there were lots of other files that were deleted, Excel files, porn, other things?

A. I am not going to say porn was part of it. But the fact is I wrote or I, yeah, I wrote in my report I believe that like you say, this drive

was formatted. Formatting a drive is the same thing as deleting every file on the hard drive. So I found, so everything is deleted. There is no such as deleted and not deleted when you format a hard drive.

Q. Did you find a reformat date before December 12, 2000, -- I mean, November 12, 2003?

A. No.

Q. You did not. Would you have expected to find them?

A. No.

Q. You would not. The, you mention that you didn't find any evidence of porn on the 120-gigabyte hard drive? I'm confused about your testimony.

A. Did I put that in my report?

Q. No. Your testimony just a short time ago. Did you testify that you didn't find any evidence --

A. That's right. And what I mean by I didn't find any porn, is I didn't find any pictures.

Q. You didn't find any pictures?

A. Right.

Q. You didn't find any recoverable video files?

A. No. All the video files that were named in a

fashion that would line up with pornography I was unable to recover.

Q. Were you able to determine that there was a lot of, that there was a shared hard drive and the existence of software programs for file sharing?

A. I was able to determine that.

Q. Okay. Did, were you able to determine that there was a substantial amount of activity with respect to that?

A. Yes, I was.

Q. Okay. And the dates and times for many of those files were during the course of the period of time from May 2003 until it was reformatted in

November 2003?

A. Yes.

Q. That's correct? That's a period of time in which Mr. Zweizig testified that it was in his fireproof safe. You found dates and times for files during that period of time?

A. Yes.

Q. Okay. With respect to the 60-gigabyte hard drive, you had mentioned that, I want to focus on e-mail activity right now. I think your testimony was there was evidence that the

60-gigabyte hard drive had been used for e-mail?
A. Yes.
Q. But the question is was it used by Mr. Zweizig for e-mail. Has it been used by Mr. Zweizig for e-mail?
A. Not that I found.
Q. Not that you found. So the question itself kind of missed the mark on that. The real question is was it used by Mr. Zweizig for his e-mail? The answer is no?
A. No. Not that I found.
Q. Not that you found. Okay. When you're examining log files for change dates, et cetera, you must have found some change dates in the log

files that you did find. What, for the, for the laptop that you examined, for the exit time e-mail, did you find any changed dates at all?
A. Actually I didn't find any changed dates at all on any of the files on any of the --
Q. For any of the computers?
A. For any of the computers.
Q. Let me ask you about the credibility of forensic scans. You had mentioned that you didn't get

the 120-gigabyte hard drive. You only received a forensic scan.

A. A forensics image.

Q. Forensic image. I'm sorry. Do you find that having a forensic image is not the same as having a hard drive?

A. Absolutely.

Q. You do believe that?

A. Yes.

Q. And the forensic, I think Mr. Cox testified that he typically travels around the country and does forensic work and it's less common for him to actually pick up hard drives. He takes forensic scans, forensic images and uses those as his tool?

A. I must have missed that in his testimony because

the way that I understood Mr. Cox is that he works in more of a E discovery business and that the data comes to him at that business and it is not always necessarily hard drives, but it could be images or it could just be data in general.

Q. Okay. But the question then with respect to a copy of a forensic image, would you say that a copy deteriorates that forensic image, is that

your position?
A. Yes. It comes down to best evidence. In some cases you will be limited to a copy, an image, not the original. Right. But the original is what every practiced forensic examiner should be going for.
Q. And with respect to the 120-gigabyte hard drive, that's all you have was the forensic image?
A. That's correct.
Q. But you found no activity of use after November 12th of 2003; is that correct?
A. That's correct.
Q. After it was reformatted, there was no evidence of activity?
A. Correct.
Q. Okay. Now, on the 60-gigabyte hard drive, that continued to be in use. So that was scanned,

forensic image was made I believe May 2005. And continued to be in use thereafter. You did a forensic, your own forensic image?
A. It was June 2005. And yes.
Q. You did your own forensic image subsequent to that date but you also had Mr. Williams'

forensic image on that date for the June 2005?

A. You say subsequent.

Q. Well you received a copy of his forensic image or received a forensic image?

A. Last weeks.

Q. That he provided?

A. Steve Williams?

Q. Steve Williams, well, the chain was Steve Williams provided it had to Mr. Cox and Mr. Cox provided it to you.

A. Okay. In that case I have received a copy of the 60-gigabyte hard drive from Steve Williams. My understanding is it was from Mr. Cox.

Q. Okay. So Steve Williams provided that forensic image which he took in June 2005 to Mr. Cox. Mr. Cox provided a copy of that to you. Okay. And that, and you evaluated that 60-gigabyte hard drive image as of June 2005?

A. Correct.

Q. And so your basis then was that in thinking back now to the volume of e-mail activity, you again to reiterate found no evidence that Mr. Zweizig used --

A. I did -- I'm sorry to interrupt.

Q. That's okay.
A. I did not do any searches for e-mail other than the exit time e-mail on the 60-gigabyte hard drive.
Q. You did not do any additional work to evaluate whether or not that, there was a volume of activity with respect to the 60-gigabyte hard drive?
A. No. Not on the one provided to me that was provided to me by Mark Cox from Steve Williams.
Q. I see. But you did on your first, on your forensic image?
A. Yes.
Q. And you found no evidence of use by Max Zweizig?
A. No.
Q. Okay. What was the, you found no use by Mr. Zweizig?
A. On the 60-gigabyte hard drive.
Q. On the 60-gigabyte hard drive. Now, on the 120-gigabyte hard drive, did you examine that

for e-mail activity for Mr. Zweizig?
A. Yes, I did.
Q. And did you find a lot of e-mail? Did you find

evidence of use?

A. I did find e-mail and evidence of use.

Q. And it was substantial?

A. I found two what they would call PST files. So storage for e-mail and they were quite large. However, they were also corrupt so I couldn't get every e-mail out of them.

Q. But you did find substantial --

A. I did.

Q. -- e-mail. And you would have expected to find substantial volumes of e-mail?

A. Yes.

Q. Okay. With respect to the floppy drive, you had indicated that on Steve Williams' report, Exhibit 71, page five, I believe, that, if you can turn to that, please.

A. I got it. No.

Q. Let's see. Exhibit 71. Maybe it's exhibit 60. Let me go there. Exhibit 68, arbitration Exhibit 68, page three, if you could go there, please. You had indicated that the date and time stamps for create date and modification

date, you reached a certain conclusion about that. Would you restate that conclusion?

A. The conclusion is that they are the exact same, so therefore it was copied, that Maxterm.doc was copied to the floppy drive not created on it originally.

Q. So it could have been, could have been drafted on this other computer and saved only one time and it would create the same statement, is that the same conclusion?

A. The conclusion is it was drafted on some other computer or a computer, saved somewhere. Now according to the, according to the document that was saved on that floppy disk, I haven't say saved, that was examined on that floppy disk, it was saved not only to a hard drive but to a floppy disk at some point in time. Just not that floppy disk that I received.

Q. You're maintaining that because these two dates are the same, you reached a conclusion and the times are the same -- Are the times on there? They are. That that represents a copy?

A. That and because it didn't contain the temp files that go along with creating or saving a file to a document to a floppy disk.

Q. So, but isn't your position that if that document was created on a computer that had a floppy drive and a hard drive, C drive, that if Microsoft Office was just brought up and that document was created, wouldn't the temp file have been on the C drive?

A. Both.

Q. It would be in both places.

A. Yes.

Q. So the temp file then, the metadata with respect to the temp file, wouldn't have been copied over to that other floppy? Is that the point?

A. No. Not the point. The temp file would not have been copied over to the other floppy disk.

Q. I see. Okay. With respect to the 60-gigabyte hard drive and the identification of the Fox Pro files you were asked to search for deleted files and you found a substantial number of deleted files after Mr. Zweizig turned over the computer. Do you recall the dates?

A. Yes. Well, I recall that it was December, I believe 29th of '03 and above.

Q. And after?

A. And after.

Q. Were you asked to look for the existence of Fox

Pro files that had date stamps prior to November 13, 2003?

A. I was asked -- No, not specifically.

Q. So you were only asked to look for deleted files, not Fox Pro files that were created prior to November 13, 2003?

A. That is correct. But I am verifying with the stipulation order. That is correct. The only, the only restriction or limit that I had for the year 2003 was the examination of media for the limited purposes of identifying records from 2003 relating to the creation, modifying, editing, storing, chain of custody, receipt and transmission of the termination letter or derivations thereof. So the actual look for destroy and tampered with files was not limited to 2003.

Q. Were you asked to examine any of Max Zweizig's computers?

A. Personal computers?

Q. Personal computers.

A. No.

Q. Laptop. He had a laptop?

A. No.

Q. And that wasn't made available to you?

A. No.
Q. And your conclusion with respect to the exit time on the e-mail was that, was that the dates and times associated with that e-mail are accurate?
A. Accurate in the sense that they were definitely sent at that date and time would be no. If you mean that the computer was accurate when it put on those date and times based on whatever the computer time was? I would say yes.
Q. Your testimony is that you have not been able to refute that evidence; is that correct?
A. That's correct.
Q. And not that it didn't happen, just that you weren't able to refute it?
A. I don't have any collaborating evidence that tells me one way or another if it's accurate or not.
MR. ROTE: Okay. That's all. Thank you.
ARBITRATOR CROW: Redirect.
Q. BY MS. MARSHALL: Yes. I just want to make sure that I understand correctly. When Mr. Rote drew the distinction between the e-mail that you testified about that, if you recall that was an

original message that was from someone else to

Mr. Zweizig, that was found by Mr. Williams on the 60-gigabyte hard drive in 2005 and his question of you was did you find any evidence that prosecute Zweizig used the 60 for his e-mail, were you drawing the distinction between receiving and sending?

A. Yes.

Q. Is that it?

Okay. So you didn't find any e-mails in which Mr. Zweizig sent an e-mail from the 60 but apparently Mr. Williams found one where he received it on the 60? Is that correct? According to his report?

A. Well, according to his report neither of those are correct.

Q. Okay. Tell me what's correct.

A. And the reason being you cannot distinctly say that number five on his report was to Max on that computer or Brent or Bret or any of the other people that were on that computer, in that original e-mail. So therefore, you can't say that he was receiving on that computer. And the same thing goes for sent. Now, I am going based

on, I would be going based on sent from him. However, even at that point there has to be a

direct file at that really tells you that it was, that it belonged to him. You cannot make the assumption that either or is delivery or activity by Mr. Zweizig.

Q. Okay. But in any case by 2008 you couldn't find that e-mail?

A. No.

Q. You were asked in cross whether you found that the 120-gigabyte had been reformatted prior to November of 2003 or prior to the November 12th date. And I believe you testified that you would not expect to find that. Why not?

A. Only because it's, it's, I don't know. It's not a usual thing to reformat the drive over and over again. Now, there are ways to check and see previous formats, but I did not run through that type of examination.

Q. Okay. But you didn't see any evidence that it --

A. No.

Q. -- had or had not been -- Okay.

A. You skipped a page.

Q. Pardon?

A. You skipped a page.

Q. I'm sorry. You're anticipating my questions?

MS. MARSHALL: I have no other questions.

ARBITRATOR CROW: All right. And you rest; is that correct? I know you have a rebuttal witness.

MS. MARSHALL: Yes, we do.

ARBITRATOR CROW: And Mr. Rote, I believe you have a witness.

MR. ROTE: One witness.

ARBITRATOR CROW: Can you get that witness on the phone now or what did you tell that witness?

MR. ROTE: I had replanned for her to be available at 2:30. I'm sorry. I thought we would take a little longer.

ARBITRATOR CROW: Do you want to see if you can get that witness now?

MR. ROTE: Let me see if I can step out.

ARBITRATOR CROW: Why don't you go give it a try. See if that witness is available. If not we'll wait until 2:30 and I have some things I