

1 ROUGH DRAFT TRANSCRIPT NOT CERTIFIED

2

3

4

5

6

7

8

9

This real-time draft is unedited and un-
certified and may contain untranslated
stenographic symbols, an occasional reporter's
note, a misspelled proper name and/or
nonsensical word combinations. All such entries
will be corrected on the final, certified
transcript.

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Due to the need to correct entries prior to
certification, this real-time draft transcript
is to be used ONLY for the purpose of augmenting
counsel's notes and is not to be used or cited
in any court proceeding or distributed to any
other parties.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

ARBITRATOR CROW: Let's go on the record.
Are we on cross-examination now?

MS. MARSHALL: In the interest of moving
this train along, I think I'm finished with
cross.

ARBITRATOR CROW: You think you're finished
with cross-examination.

Any redirect, Mr. Rote?

MR. ROTE: A few questions.

ARBITRATOR CROW: All right.

- Q. BY MR. ROTE: There's been a suggestion that
it's possible to have copied files from hard
drive or from another flash drive or something
of that nature over to the 120-gigabyte hard
drive after that was reacquired by NorthWest.
If that had been done how would that have
created affected the created date or
modification date of each of these files?
- A. My understanding just knowing how we're talking
about the file sharing issues that we saw on the
120-gig drive and the e-mail and some of the
other things to show that it had been in use for

♀

1
2

a period of time, at least up until, to
regular use up until May of 2003 When The drive

11-5-10

3 was removed from the Sony Vairo. After that
4 point, if someone wanted to do, put a
5 substantial amount of material on that hard
6 drive and make it look like it came from a time
7 period, since we're talking about movie
8 downloads and TV downloads, someone would have
9 to take that drive, put it into another computer
10 as the secondary drive, or, you know, copy tons
11 of material off onto their own computer and then
12 copy it off onto this drive or save it directly
13 to that drive however you want to get it to that
14 120 drive and you have to constantly redate your
15 computer to get different dates on that file to
16 make it look like it came from 2003 when you're
17 actually doing it in say 2004, 2005 if you want
18 to make that jump. They are wreck Lee it's
19 possible. It would be, in my opinion, as a
20 practical matter, it would not be feasible just
21 because of the sheer amount of data that you
22 would have to put on there, you'd probably have
23 to have someone working full time to do that
24 kind of a job in order to make it look like
25 something else. And as I looked at the contents

♀

4

1 of that drive and I believe Mr. Cox said the
2 same thing, is that it looked to me, all things
3 being equal, is if that drive up until May of
4 2003 was used for what it was intended for, is
5 for the NorthWest Direct work, it had the

11-5-10

6 e-mail, it had the files, and then at some point
7 and Mr. Cox can clarify that, if we need to,
8 there was a lot of file sharing going on, a lot
9 of files were downloaded. It appeared that that
10 happened most likely during the time frame that
11 the drive was, would have been before Mr. Rote
12 picked it up.

13 Q. Okay. But let me make this point clear though.
14 If you had, from a hard drive or another flash
15 drive or something of that nature and you wanted
16 to copy a thousand files over and you copied
17 them all at the same time, they wouldn't have
18 all the different created dates, modification
19 dates. They would be copied with the copy date?

20 A. They would, one of the dates for each of those
21 files, they would all share the same date. At
22 least one. Whether it was the file created
23 date, the file modified date the last written
24 date, one of those dates and times they would
25 share in common.

♀

5

1 ARBITRATOR CROW: I'm not sure I understand
2 that.

3 THE WITNESS: If, I can clarify. If you
4 copied a file, say you have a file on a thumb
5 drive and it has a date of just pick January 1st
6 of 2010 at 10:00 in the morning. If you copy
7 that, put it into a computer and copy that over
8 to your hard drive, it's going to still have

11-5-10

9 that January 1st of 2010 date and time on it as
10 one of the date and time stamps. Files all have
11 multiple date and time stamps involved in it.
12 It's going to have that as one of its dates and
13 time stamps. Then it's going to have a new date
14 and time for when you save it to the new
15 computer. So if I take a block of a thousand
16 files off of this other media and I save it in
17 mass to my computer, it's going to have the same
18 date and time when I copied it over.

19 ARBITRATOR CROW: The original date or the
20 new date?

21 THE WITNESS: It's going to have a new date
22 on there.

23 ARBITRATOR CROW: Going to have two dates.

24 THE WITNESS: Well, most files have at least
25 three or four dates attached to them, a created

♀

6

1 date, a last access date which is when someone
2 maybe opened it and closed it. It's going to
3 have a last written date, which means, a last
4 written and last modified. And there are some,
5 they're not always the same depending on the
6 files and how they're used. Sometimes, I can
7 look at a file and say, okay, the last written
8 date appears to be when it was saved to this
9 computer. The created date matches when it was
10 originally saved to its original media. That's
11 not always the same with every file in every

11-5-10

12 operating system. It's one of the oddities
13 about Microsoft Windows.

14 ARBITRATOR CROW: And how does that relate
15 to the 120 hard drive as it was when it was
16 turned over to NorthWest Direct?

17 THE WITNESS: When it was turned over to
18 NorthWest Direct, the drive, which has two drive
19 letters on it, C and D, so there's two
20 partitions so it would look like two separate
21 drives in a computer, both of those have been
22 reformatted. So they're essentially new open
23 blocks to have data saved to it. It had, if you
24 plugged it in and looked at it, it would say no
25 data. And it had the new partitions, the time

♀

7

1 it was formatted appeared to be just prior to
2 when Mr. Rote said he went and picked up
3 computer and the hard drive from Mr. Zweizig.
4 So at some point, that was in a computer. A
5 computer was set to that date and that time.
6 And I'd have to look back up and see the
7 specific time. I believe it was something like,
8 sorry, I have to look back here real quick,
9 November 12, 2003, the first partition C had a
10 date of 11:26 a.m. and the D partition had
11 12:31 p.m. so it happened, it happened in about
12 an hour's time period, those two drives were
13 reformatted. Whatever was on there before then
14 becomes an allocated space. It's just data

11-5-10

15 that's still out there that can be written over
16 but it can still be recovered. And all of that
17 data showed a substantial amount of activity.
18 And the way when I looked at it, that activity
19 for the NorthWest Direct material and the
20 e-mails had all come to pre, before May 2003
21 When The drive was removed from the computer and
22 set aside.

23 Now my understanding since then through
24 Mr. Cox and Mr. Rote was that the, a lot of the
25 file sharing activity was dated to that mid 2003

♀

8

1 time period, indicating the drive was still
2 being used arch it had been removed from the
3 Sony Vairo. I can't corroborate that myself
4 because I didn't see that, I didn't look for
5 that myself but I did see a substantial amount
6 of file sharing activity that appeared that
7 files were being downloaded through a file
8 sharing program onto that computer and that
9 these dates of those files was over an extended
10 period of time, rather than a single time frame
11 that would indicate all those files being copied
12 at once onto the drive.

13 ARBITRATOR CROW: All right. Mr. Rote.

14 Q. BY MR. ROTE: Exhibit 146.

15 ARBITRATOR CROW: Do you have one,
16 Ms. Marshall? Did you get one?

17 Q. BY MR. ROTE: This is an e-mail, you see

18 Exhibit 146, page one. There's been some
19 discussion about not having access to a
20 substantial number of drives or timely access to
21 a substantial number of drives. Have you had an
22 opportunity to review any hard drives from
23 Mr. Zweizig?

24 A. No. I didn't, other than the computer and the
25 hard drive that belonged to the company, I

♀

9

1 didn't have a chance to see any of his personal
2 computers.

3 Q. Down below on this e-mail you see an e-mail from
4 Max Zweizig identifying the machines on which he
5 needed the registration code for a particular --

6 ARBITRATOR CROW: What page are you looking
7 at, Mr. Rote?

8 MR. ROTE: Page one.

9 MS. MARSHALL: You may need to speak a
10 little bit louder so that it can be heard on the
11 phone here.

12 Q. BY MR. ROTE: Okay. Down under the original
13 message from Max Zweizig you see that there are
14 serial codes needed, the registration codes
15 needed for particular machines that he was
16 having access to. Do you see, do you see
17 that --

18 A. Yes, I do.

19 Q. -- on page one? And do you see that he's
20 identified his laptop?

- 21 A. I do below the NWT machine.
- 22 Q. And would that lead to you conclude that he was
- 23 using his laptop for company business?
- 24 A. It appears that he has, there's at least one
- 25 other machine that is, that is one that I did

♀

10

- 1 not have access to.
- 2 Q. All right. Let's go to page two. This is
- 3 discovery provided by Mr. Zweizig. Up at the
- 4 top of this page there is an identification
- 5 called Maxz@erols.com.
- 6 A. Yes.
- 7 Q. Can you tell us what that represents.
- 8 A. When you're seeing an Outlook program or Outlook
- 9 express, the Microsoft e-mail program, when you
- 10 print out your e-mails, if you're to view an
- 11 e-mail printed out it puts the e-mail address
- 12 you've put into the program at the top of that
- 13 e-mail. So this would appear to have been
- 14 printed from an e-mail program where the
- 15 Maxz@erols.com was the address used.
- 16 Q. The text of the e-mail however has the e-mail
- 17 from Max as Max@NWtelmarketing.com. So you
- 18 presume what from this?
- 19 A. Well, this is hard to say. It's, without doing
- 20 some further research on my parts, typically if
- 21 you've got your Outlook set to receive, send and
- 22 receive e-mail with the one address, the
- 23 Max@NWtelmarketing.com, I would expect to see

11-5-10

24 Max@NWtelmarketing.com at the top. But I don't
25 see that. So it indicates that maybe something

♀

11

1 else has happened with this e-mail. Maybe it
2 has been forwarded to the erols.com address or
3 in some way opened up within that program with
4 that profile.

5 Q. Nonetheless, this e-mail was provided and copied
6 from a source that was an account called
7 Maxz@erols.com?

8 A. It does appear that way, yes.

9 Q. Would you go to page three. Same conclusion for
10 page three?

11 A. It looks the same, yes, the same headers.

12 Q. And that, of course that date for that e-mail is
13 October 1st, 2003.

14 A. Yes.

15 Q. Okay. Go back, we have just similar examples on
16 page four. This is dated on page 4,
17 October 2nd, 2003.

18 A. It does look like that way, yes.

19 Q. And that is referring to a do not call
20 complaint, do you see that?

21 A. Yes, I do.

22 Q. And then on page five also at the top of the
23 page, the same account named Maxz@erols.com?

24 A. Yes.

25 Q. And the date on that e-mail is November 13,

♀

12

- 1 2003?
- 2 A. That's correct.
- 3 Q. Okay. And the same for page six?
- 4 A. Yes.
- 5 Q. Same for page seven?
- 6 A. In that case it's a message from your e-mail
7 address to Maxz@erols.com and there's no
8 NorthWest, no company e-mail address on that one
9 at all.
- 10 Q. So this page seven is different from the other
11 ones because it was actually sent to
12 Maxz@erols.com?
- 13 A. It appears that way, yes.
- 14 Q. So but the other, in relationship to the other
15 e-mails, then all of these other e-mails were
16 also kept in the Maxz@erols.com folder?
- 17 A. It looks like it, yes.
- 18 MR. ROTE: That's all the redirect I have.
- 19 ARBITRATOR CROW: I think you opened some
20 new areas if you wish to cross-examine,
21 Ms. Marshall, on these issues, you may do so.
- 22 Q. BY MS. MARSHALL: Just a couple questions.
23 Mr. Williams, were you aware that the company
24 widely used a program called PC anywhere?
- 25 A. I wasn't aware of that, no.

♀

- 1 Q. Okay. Well, you're familiar with that program,

- 2 weren't you?
- 3 A. Somewhat, yes. I've never used it myself or
4 done any research on it.
- 5 Q. So, if, for example, Mr. Zweizig were out of the
6 office, were in some other office or traveling
7 and needed to pick up his e-mails, wouldn't it
8 make sense to you that he would take his laptop
9 with him, not his desk top?
- 10 A. That would make certain PC Anywhere allows for
11 remote access of another computer through a
12 different computer.
- 13 Q. Okay. And were you familiar with the ISP
14 service used by, at NDT?
- 15 A. No, I was not.
- 16 Q. Okay. Well, you're familiar with ISP services
17 where you can actually call, or dial up over the
18 internet and get your e-mails remotely?
- 19 A. Through a web page, yes.
- 20 Q. Through a web page. Okay. And were you aware
21 that NDT had such a service?
- 22 A. No. It's a common practice. My department for
23 the City of Eugene has the same service where I
24 can access my e-mail remotely from any computer
25 through a web page.

♀

- 1 Q. So in either case, if Mr. Zweizig was either
2 accessing e-mails remote Lee or accessing them
3 over the internet using his laptop computer, for
4 example, if he's out of the office, if he's

5 traveling, something like that, and he prints
6 it, it would be printed off of the
7 Maxz@erols.com; right?

8 A. It could be. I don't know the format. I know
9 that looking at this format it looks like
10 Outlook the way Outlook prints when I print my
11 e-mails directly from my work computer rather
12 than the format when I print them remotely, but
13 I don't know for sure as how that would look.

14 Q. You don't know how Mr. Zweizig's computer was
15 set up?

16 A. No, because I've never seen his computer.

17 Q. Okay. But you do know that all of these
18 documents that you've seen here, Mr. Zweizig
19 produced in this litigation. Those have his
20 Zweizig number at the bottom of them; right?

21 A. Yes. That's my understanding.

22 MS. MARSHALL: Okay. That's all the
23 questions I have.

24 ARBITRATOR CROW: Are you finished with this
25 witness?

‡

1 MR. ROTE: Yes, we are.

2 ARBITRATOR CROW: All right. You may be
3 excused and don't go back to Eugene and arrest
4 any Oregon football players, please.

5 THE WITNESS: I can't guarantee that because
6 that's where I'll be all day tomorrow.

7 ARBITRATOR CROW: Thank you for coming.

8 THE WITNESS: Thank you, sir.

9 ARBITRATOR CROW: Next witness, Mr. Rote.

10 Are you putting on another expert or one by
11 telephone?

12 MR. ROTE: No other experts. The person by
13 phone will be available at 1:00.

14 ARBITRATOR CROW: All right. That's fine.

15 MS. MARSHALL: All right. That's fine.

16 Then we would like to call Mr. McAnn.

17 ARBITRATOR CROW: All right.

18 MS. MARSHALL: And what I would suggest is
19 that he come up here so that he's close to the
20 phone and close to you. And he also has some
21 equipment with him that would allow him to
22 actually show you some of the things that he's
23 going to describe.

24 ARBITRATOR CROW: All right. And do you
25 want to sit next to him then or do you want to

♀

16

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

2 MS. MARSHALL: I'll move right next to him.

3 He can turn and talk to you.

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

6 THE WITNESS: Yes, sir.

7 ARBITRATOR CROW: Thank you.

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

10 ARBITRATOR CROW: Take your time. Let's go

11 off the record while he's setting up and you can
12 relax.

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

14 ** ** sworn sworn ** **.

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

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

♀

17

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

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

12 A. I do.

13 Q. What is that?

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

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

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

♀

18

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

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

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

15 Q. Okay. And you've brought a curriculum vitae
16 with you, which I have a copy for you and for

17 Mr. Crow. And did's a petty detailed CV so I
18 won't have you go through it in detail. But I
19 notice in your CV that you also, in addition to
20 working full time for *PACR and doing consulting
21 that you've just described, that you also are,
22 that you teach the subject.

23 A. That's correct.

24 Q. Can you just give Mr. Crow an idea of what your
25 teaching experience is?

♀

19

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

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

14 A. I have. Well, I've done writing that I have
15 developed into videos, video tutorials, how to
16 forensics for certain things such as incident
17 sponsor hacking, like compromises on servers to
18 general forensics, et cetera. So I've created
19 at least ten different videos that are posted

20 out on the internet sort of like the U-Tube era
21 for experts such as ourselves to go study and
22 watch and learn from.

23 Q. Okay. And have you also been a coauthor of
24 publication?

25 A. I'm currently working on an advanced forensics

‡

20

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

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

11 A. Okay. Well, it's sort of across the board
12 another gambit. I specialize Encase, which has
13 been utilized with some of the other experts
14 here. I specialize in FTK. I also have a lot
15 of knowledge about open systems. So open source
16 software, other software such as X-Ways
17 Forensics, Smart, a lot of different forensic
18 software that's out there. And the reason I do,
19 the reason I'm involved in those is because I
20 have more, I have a lot of experience in not
21 just Windows but UNIX as well as well as
22 networking and applications. So my, I try to

23 say that I'm the jack of all trades but not
24 quite the master of all or none, I say. Sorry.

25 Q. Have you, has your testimony been accepted as

‡

21

1 expert testimony in federal court, for example?

2 A. Yes, it has.

3 Q. Here in Oregon?

4 A. Here in Oregon.

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

7 A. Yes, it does.

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

10 A. I am.

11 Q. Including Microsoft Outlook?

12 A. Very much so, yes.

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

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

18 Q. Okay. And have you performed in other cases
19 involving issues that involved the deletion of
20 matter or wiping matter or somehow hiding items
21 in computer environment?

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

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

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

19 Which do you see yourself as?

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

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

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

10 A. Absolutely.

11 Q. Have you served as a special master before?

12 A. Yes, I have.

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

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

♀

24

1 Mr. Williams was talking about earlier that may
2 or may not change. That's file system metadata.

3 And then there's application metadata. And that
4 is like if you have your Microsoft Office, you
5 open up a Word document, you know, your Word
6 document stores things like the author, the
7 company, how many words or characters are in the
8 document itself when it was last printed,
9 et cetera. There's a lot of data that's stored
10 within the document itself, which becomes --

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

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

15 ARBITRATOR CROW: No. No. I'm more
16 concerned with those fingers over here. Go
17 ahead.

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

22 Q. BY MS. MARSHALL: Okay.

23 ARBITRATOR CROW: I understand.

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

♀

25

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

5 A. Well, the metadata both file system and

6 application metadata can have and will have a
7 created date and several other dates involved.
8 You can try to --

9 ARBITRATOR CROW: On the document itself?

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

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

23 THE WITNESS: Which page?

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

♀

26

1 at 9:35 a.m.

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

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

11 THE WITNESS: You will all recognize this.
12 I'm not going to actually send it. But I am
13 going to create a new e-mail and this is
14 Outlook. This is also, I should mention that
15 this computer is tuned so it's Outlook XP,
16 office XP just like what existed when this data
17 happened when all the data was being utilized.

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

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

23 THE WITNESS: That is correct.

24 ARBITRATOR CROW: All right.

25 THE WITNESS: Now there's other application

♀

27

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

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

8 THE WITNESS: Yes.

9 ARBITRATOR CROW: From the computer?

10 THE WITNESS: Yes, I am.

11 ARBITRATOR CROW: The hard drive; is that

12 correct?

13 THE WITNESS: Yes, sir.

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

16 Go ahead.

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

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

♀

28

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

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

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

7 THE WITNESS: Yes, sir.

8 ARBITRATOR CROW: All right.

9 Q. BY MS. MARSHALL: Okay. And what would you look
10 at on the hard drive to determine if a date had
11 been changed?

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

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

- 15 to do that?
- 16 A. No. When it comes to e-mail anyway, e-mail you
17 could also refer to the internet service
18 provider that the e-mail went through if the
19 e-mail went through an internet service
20 provider.
- 21 Q. Okay. With respect to a paper document, for
22 example, the letter that's at issue in this
23 case, would you have to refer to the hard drive
24 in order to examine the logs?
- 25 A. Yes.

♀

29

- 1 Q. Okay.
- 2 ARBITRATOR CROW: Give me that one again,
3 Linda, that question again.
- 4 Q. BY MS. MARSHALL: I asked whether with respect
5 to the written document, the letter in this
6 case, would he have to examine the hard drive in
7 order to, examine the logs on the hard drive in
8 order to verify the date and time?
- 9 ARBITRATOR CROW: And the answer is no?
- 10 THE WITNESS: To, since she, since she
11 clarified the question, the answer is that log
12 files, I utilize log files to validate dates and
13 times. But to validate an actual date and time
14 from a piece of paper that was printed or used
15 on a computer, then I have to go into the file
16 system and the applications and configuration on
17 the hard system. So the hard drive is the

18 answer is yes, I absolutely need the hard drive
19 to validate that document.

20 ARBITRATOR CROW: All right. Thank you.

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

♀

30

1 litigation hold?

2 A. Absolutely. So a litigation hold is where one
3 or both parties understands that litigation is
4 going to be occurring and whatever the
5 allegations are, any evidence involved in that
6 litigation must be held, meaning it must be set
7 aside and untouched during the time of that
8 litigation.

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

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

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

21 THE WITNESS: Yes, you could.

22 ARBITRATOR CROW: All right.

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

‡

31

1 image; is that correct?

2 A. That is correct.

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

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

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

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

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

23 A. Yes. So spoliation is the intentional or even

24 unintentional change or manipulation of data
25 that may be in that litigation hold. It could

32

1 be the accidental deletion of a file, it could
2 be the accidental overwritten file or it could
3 be the loss of data or the loss of a data
4 storage device itself.

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

7 A. Yes, they have.

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

10 A. Absolutely.

11 Q. Do you teach them about spoliation?

12 A. Yes.

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

15 A. Yes, I have.

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

17 A. Yes, they have.

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

23 A. And Mr. Rote's.

24 Q. And Mr. Rote's computer.

25 A. Yes.

33

1 Q. Do you have available to you the forensic tools
2 that were available? For example, the ones that
3 Mr. Williams was using?

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

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

10 A. Yes, I have.

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

17 A. Newer or not.

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

19 A. You got it. Correct.

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

22 A. So let's start with FTK.

23 ARBITRATOR CROW: D or --

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

♀

1 more towards the technician side of a forensic

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

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

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

‡

1 both of those products.

2 Q. Okay. I'd like to have, I'd like to move right
3 into one of the, one of the important issues in
4 the case, and that's the e-mail that's at issue.

- 5 And I believe it's Exhibit 14. I'll let you
6 take a look at it. And I'll just ask you
7 whether I have asked you to do forensic
8 examination with respect to the, to this e-mail.
9 A. Only in respect to the latest protective order.
10 Q. Yes.
11 A. Have I taken a look at this e-mail and examined
12 it forensically.
13 Q. Okay.
14 A. I'm sorry. Let me add onto that. The prior,
15 the prior stipulation, protective order, I found
16 this e-mail but it wasn't in the stipulation for
17 me to really bring it out and examine it fully
18 like I have since the new protective order came
19 out.
20 Q. Okay. Well, let's go back to the first time
21 that you approached the subject of the e-mail.
22 And first of all, what computer did you
23 understand the e-mail was created on?
24 A. My understanding is it was created on Mr. Rote's
25 laptop.

‡

- 1 Q. Okay. And were you provided Mr. Rote's laptop
2 for examination?
3 A. Yes, I was.
4 Q. Okay. When were you provided his laptop?
5 A. I believe it was December 12th, 2008. And if
6 you don't mind, I'm going to grab my folder down
7 there.

8 ARBITRATOR CROW: December 8th?

9 THE WITNESS: Yes.

10 MS. MARSHALL: December 12, 2008.

11 THE WITNESS: I am going to refer to, for
12 this I am going to refer to my report that I
13 submitted. I don't know which exhibit it is.

14 MS. MARSHALL: It is an exhibit, I believe.
15 While you get it out I'll get the report number.

16 THE WITNESS: So to continue with that, I
17 was, I was, did you handed over?

18 Q. BY MS. MARSHALL: You were provided. Were you
19 provided the actual laptop?

20 A. I was provided the actual laptop on December
21 12th, 2008.

22 Q. Okay. And the date of the e-mail is what?

23 A. October 2nd, 2003.

24 Q. Okay. So you were looking at the forensic data
25 roughly five years after the, ostensibly after

♀

37

1 the e-mail?

2 A. Can you repeat the question, please.

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

6 A. That is correct.

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

9 A. I was actually in this building. I can't tell
10 you which floor, but, or which law firm it was,

- 11 but the name of the attorney was Jeff Edelson.
- 12 Q. Okay. So you, your office is in Seattle?
- 13 A. Yes.
- 14 Q. Is that correct? So you came down here
- 15 specifically to examine or to take images of the
- 16 relevant computers?
- 17 A. That is correct.
- 18 Q. Okay. Can you tell us the general condition of
- 19 the laptop at that point?
- 20 A. The laptop physically did not look damaged.
- 21 Q. And what did you find when you went to take an
- 22 image of it?
- 23 A. What I found is that the hard drive itself,
- 24 however, did appear physically damaged, not from
- 25 the outside but by the sounds and its

♀

38

- 1 performance that it had when I was attempting to
- 2 take a forensic image, such as whining and
- 3 almost a grinding sound inside a hard drive,
- 4 smug would hopefully never want to hear unless
- 5 you backed up all of your files.
- 6 Q. Okay. We should have probably done this
- 7 earlier, but when you say you take an image,
- 8 what are you really talking about?
- 9 A. So what that means, and actually I'm going to
- 10 grab my bag for this. What that means is that
- 11 there's a procedure, procedure that I utilize in
- 12 order to preserve the evidence. And this
- 13 procedure first off starts off with me

14 documenting what the evidence is and the
15 documentation comes in three forms. It comes in
16 writing it down, as an example. I have these
17 forms that I fill out when I go on site and I
18 actually look at the equipment and take the
19 equipment. So I'm writing down serial numbers
20 and model numbers, et cetera. The second is the
21 chain of custody. And the third is actual
22 pictures. So I take a camera along with me and
23 take pictures. Equipment so I can tell what
24 state it was in, I can tell how it was
25 configured and I take up close macro shots of

♀

39

1 the serial numbers. This is how I keep from
2 accidentally not being able to read my own
3 handwriting.
4 Q. All right. So when you say an image, now the
5 other two gentlemen have talked about images,
6 too. What is, what is an image?
7 A. So after I have documented everything that I
8 need to, that I feel that I need to, I do what's
9 called a forensic image, taking a forensic
10 image. It's a bit by bit or byte by byte,
11 depends on how you want to say it, copy of a
12 data storage device. And that data storage
13 device can be a hard drive or a floppy disk or a
14 CD rom or anything. It can be an i-Pod or
15 what's inside an i-Pod I should say. So what
16 happens is that most of the scenarios,

17 especially computers and with their hard drives,
18 we hook them up to what's called a write-blocker
19 device. It's a piece of hardware. And the
20 reason why we use a piece of hardware is as to
21 things like viruses don't affect us. If my
22 computer here gets affected and I'm using a
23 software device in order to keep from writing to
24 a hard drive, it's possible that that virus has
25 taken over and changed it to where I can

♀

40

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

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

18 A. That's correct.

19 Q. Is that it?

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

22 A. That is also correct.

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

‡

1 A. No.

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

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

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

16 A. I was able to complete the image after multiple
17 tries, since it was physically damaged, and,
18 however, the software that we utilize goes
19 through and if it has trouble reading any part
20 of the drive, it records it but it marks it all
21 as zeros. So I can't actually get access to the
22 data, wherever those bad areas were. And again,

23 I actually tried imaging this drive five times
24 during the course of the period that I was at
25 this, at Jeff Edelson's office.

‡

42

1 ARBITRATOR CROW: The laptop.

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

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

15 A. The longer and longer that hard drive or data
16 storage device is kept in service, the more data
17 that is deleted is overwritten. You know, the
18 more it fills up, the less of a chance you have
19 of recovering deleted files.

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

22 THE WITNESS: That is correct.

23 ARBITRATOR CROW: All right.

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

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

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

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

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

11 A. Referring back to my report.

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

15 ARBITRATOR CROW: I think it is.

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

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

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

- 1 I took the image and I had this in my hands.
- 2 Q. BY MS. MARSHALL: Okay. In your judgment when
3 should the litigation hold have gone into effect
4 for the hard drive that this exit time e-mail
5 was created on?
- 6 A. In my opinion, the moment whomever initiated the
7 litigation, you know, began to think about the
8 litigation and/or discuss the litigation with an
9 attorney.
- 10 Q. Okay. And is this an example of what you were
11 talking earlier about, spoliation, what can
12 happen if the litigation hold is not put into
13 effect?
- 14 A. Absolutely. The fact that these were in use for
15 years arch the litigation was put into effect is
16 unintentionally overwriting data, which is
17 spoliation.
- 18 Q. Did it prevent you from doing what you needed to
19 do in order to properly examine the hard drive
20 for this e-mail?
- 21 A. In several instances. A lot of, especially if
22 we're talking about just the e-mail, this e-mail
23 that was, to exist, you know, it's possible that
24 copies or original drafts, et cetera, existed on
25 this laptop at one time but I was unable to

♀

45

- 1 discover because of the overwritten data.
- 2 ARBITRATOR CROW: Well, let me ask you this,

3 as I understand your earlier testimony, you can
4 determine from the hard drive whether the date
5 on the computer has been manually changed.

6 THE WITNESS: That is true.

7 ARBITRATOR CROW: Can that information be
8 overwritten?

9 THE WITNESS: Absolutely.

10 ARBITRATOR CROW: All right.

11 THE WITNESS: Log files generally will do
12 what they call rollover. So they can only go,
13 get up to a certain size and then after that
14 size is met, then they start overwriting the
15 date that's in the beginning of it. It's also
16 very similar to how the hard drive works when it
17 deletes data.

18 ARBITRATOR CROW: All right.

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

21 A. Yes, it did.

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

24 A. Yes, I have.

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

♀

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

3 A. June of 2005.

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

- 6 A. That was actually last week, last Tuesday. And
7 the date skips my mind. So you'll have to fill
8 that in for me. Actually I can fill it in.
9 Tuesday, October 26th.
- 10 ARBITRATOR CROW: Okay. You examined it --
11 THE WITNESS: No. I received it.
12 ARBITRATOR CROW: All right. And this is an
13 image taken in June 2005.
14 THE WITNESS: By Steve Williams.
15 ARBITRATOR CROW: All right.
- 16 Q. BY MS. MARSHALL: So this is 2010 and we're in
17 the middle of the arbitration. And is this the
18 first time that you have been able to examine
19 the computer as it was in 2005?
20 A. Yes.
21 Q. And even then it was a year and a half after the
22 fact; is that correct?
23 A. That is correct.
24 Q. Okay. And first of all, did receiving this
25 image, even though you now have it, did that, in

♀

47

- 1 your view did that put Mr. Zweizig at a
2 disadvantage?
3 A. Yes, because that year and a half is still, and
4 the fact that the drive is so small, being a 10
5 gigabyte drive, that far back, the data that's
6 being overwritten happens even faster than a
7 drive that is bigger.
8 Q. Okay. So when you examined Mr. Williams' image

- 9 of the laptop, did you find missing or data that
10 was, or did you find that data was missing that
11 you would have hoped to have seen there?
- 12 A. Are you asking did I find data that I didn't
13 find when I took my own image?
- 14 Q. Let me rephrase the question. Did you, in
15 looking at the image of the laptop that
16 Mr. Williams took, was there data missing that
17 you would have hoped to have seen that you
18 attribute to overwriting, et cetera?
- 19 A. One example, and there are many more, would be
20 the log files. The idea is that, when I
21 originally had access to this computer, not only
22 was there an e-mail, you know, or e-mails about
23 the termination, but there was a letter about
24 the termination. And I was unable to find that
25 information on the computer. That was before

♀

48

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

6 ARBITRATOR CROW: Well, to overwrite at the
7 change of a date, manually, would you have to
8 manually change the date? I mean, is that, do
9 you overwrite the change of a date by change
10 being the date again.

11 THE WITNESS: Yes, you can.

- 12 ARBITRATOR CROW: Is that the only thing
13 that would overwrite the change of a date?
14 THE WITNESS: No.
15 ARBITRATOR CROW: What else would.
16 THE WITNESS: There are programs that can.
17 ARBITRATOR CROW: All right. Go ahead.
18 Q. BY MS. MARSHALL: Okay. In addition to
19 examining Mr. Williams' forensic image, which I
20 take it you're primarily relying upon now; is
21 that correct?
22 A. As of a few days ago, yes.
23 Q. Okay. Did you review his report?
24 A. Yes, I did.
25 Q. Okay. And that would be Exhibit 68. And we

♀

49

- 1 will be referring to that quite a bit?
2 ARBITRATOR CROW: 68?
3 MS. MARSHALL: Exhibit 68, is a report that
4 Mr. Williams prepared in 2005 relating to his
5 examination of the laptop.
6 Q. BY MS. MARSHALL: Let's see. You need to have
7 Exhibit 68 in front of you. And we have the
8 books down here, I guess.
9 A. Is it okay if I pull it up on my computer
10 instead?
11 Q. Sure. If you have that on your computer, that's
12 fine?
13 A. I believe that was Exhibit 5, NWD 0005 before;
14 right?

11-5-10

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

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

25 ARBITRATOR CROW: Would I do it the same as

♀

50

1 I would change the time, use that same?

2 THE WITNESS: Simply by double clicking on
3 the clock in the corner, that's exactly how you
4 change the date.

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

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

10 A. That actually will change, not necessarily
11 change, but that will impact the file system
12 metadata as well as the document metadata. As
13 an example, the dates and times that we're
14 looking at in this exhibit, that's application
15 metadata. That's metadata that Outlook,
16 Microsoft Outlook has put into this e-mail. So
17 by changing a date you could, well I mean

11-5-10

18 demonstrate this. And I already have, in a way,
19 if I change my date from right now I actually
20 have it dated until tomorrow. Let's say I
21 change it to November 1st of this year, this
22 month, okay, I set my date back just by double
23 clicking as you are aware of changing your time,
24 correct. Now whenever I, if I create a new
25 e-mail and I can make this to anybody, I'll send

♀

51

1 it to Max, what was it Erols, E R O L S. I
2 think I spelled it wrong but it doesn't matter.
3 Test e-mail. All right.
4 Q. Now, before you go any further, can I ask you,
5 do you have to be hooked up to an internet in
6 order for this to, this demonstration to work?
7 A. No.
8 Q. Okay. So you're not depending on any outside.
9 So this is all within the computer; is that
10 right?
11 A. That's correct.
12 Q. Okay. So why don't you show us what happens to
13 the date and time that you just made the change
14 to.
15 A. Okay. Once I send this, it's going to write a
16 couple different dates, three different dates
17 actually. It's going to write creation date, a
18 receive date and what's called a sent date or a
19 submit date. The submit date actually will not
20 happen because as you can see here it is sitting

11-5-10

21 in my out box. But it will have a fourth date
22 called a modification date. And that you will
23 see back on the exhibit, so what I just did is
24 going to create this creation date, a delivery
25 date and pay a modification date.

♀

52

1 ARBITRATOR CROW: But not a submit date.

2 THE WITNESS: Not a submit date. Not yet.

3 ARBITRATOR CROW: All right.

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

6 A. Okay.

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

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

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

13 A. Yes.

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

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

24 waits for it to be officially submitted.

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

53

1 saved?

2 A. Yes.

3 Q. Okay. So if you save it rather than, if you
4 don't, let's say you don't send it at all, you
5 close and it asks you do you want to save it and
6 you say yes, that would, that would create a
7 delivery date also?

8 A. Yes.

9 Q. Okay. Now, there's some discussion about this
10 submit date. Okay. And as to whether that is
11 when somehow the e-mail bounces off of an ISP or
12 something like that. And you recall
13 Mr. Williams' testimony about that?

14 A. Mr. Williams' testimony was he thought that the
15 submit date was received back from the server,
16 like a response once you send it out. In truth,
17 the submit date is put into place the same as
18 automatic the other dates by the application,
19 not by the outside ISP or a server of some sort,
20 for the sender. I want to be specific. That's
21 for the sender. It does not receive that send
22 date or that submit date by an ISP. A
23 recipient, however, a recipient of that e-mail
24 will receive a date, one of these dates will be
25 changed and applied by an ISP. But in this case

54

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

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

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

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

16 THE WITNESS: Uh-huh.

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

20 THE WITNESS: Only on the recipient side.

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

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

♀

1 ARBITRATOR CROW: All right. Am I getting

2 ahead of things? I'm sorry.

3 MS. MARSHALL: Yes.

4 ARBITRATOR CROW: I apologize.

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

13 A. Yes, I can.

14 ARBITRATOR CROW: I assume you can.

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

19 A. And the only true way of doing that forensically
20 is by being able to analyze logs to seem if the
21 changes were ever made. And if you don't mind
22 I'm going to demonstrate this as well. I've
23 changed my date on this computer several times.
24 And I happen to be logging my firewall, the
25 network. So the network connectivity that's

♀

1 been going on with this laptop since I've been
2 at home, since I've been here on the wireless
3 network here, it's been logging to a log file on
4 my desk top here. And this log file is the

11-5-10

5 firewall log file. What you are going to see
6 here say log file writes sequentially. It
7 doesn't care what the date is. It doesn't care
8 anything. It's going to keep writing it one
9 line by line. And it doesn't sort by anything.
10 So as you change your date you'll notice, I'm
11 going to light it up here, you'll notice that I
12 went from 10-26-2010 to 10-26-2003 back to
13 10-26-2010. Right. That's, so I can tell when,
14 by analyzing log files when somebody changed
15 their date and time. And I mean, and you see
16 this log file is very big, but you can see that
17 the changes are still there and it, again,
18 you'll see I went from here 10-05, October 5th,
19 2010, to October 5th, 2003. It doesn't have to
20 be just a year. It can be any date any time
21 that I change and I will see the difference in a
22 log file.

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

♀

57

1 anybody had, during that period of October of
2 2003, say, through October, or through May of
3 2005, whether anybody had tampered with the
4 internal clock?

5 A. Only if I get to the log files in time. Before
6 they get overwritten. This one happens to be
7 set for 32 megabytes. So after it's written

8 32 megabytes, it's going to start to overwrite
9 everything in the beginning. Most of them by
10 default, this is only set to four megabytes. So
11 after a long time, especially with a 10 gigabyte
12 drive, this information will get overwritten
13 before I got a chance to examine it.

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

20 A. Yes. An example would be usage. If you were
21 going to do an investigation about the activity
22 on a computer, I don't know if we can find it,
23 but in one of the exhibits that Steve Williams
24 has wrote in his report, he shows a timetable
25 that Encase is able to produce. So it shows

♀

58

1 that on yesterday so many files were written to,
2 so many files were accessed, so many files were
3 modified, et cetera. All right. So many files
4 were created. It's a timetable in one of his
5 exhibits and I don't know which one or if we
6 have the ability to find it quickly. However,
7 that timetable can say, let's say if you have, I
8 wish we could draw here. If you have a square
9 for a day of every week, let's look at the
10 squares on this wall. Okay. So we have and

11 we'll count that one as seven over there. All
12 right. So if you have a square and this is a
13 big timetable of each one in the seven days in
14 it, you know, if something is empty, if one of
15 these squares is empty, then in a timetable the
16 assumption is if the square is empty that the
17 computer was not accessed or turned on during
18 that day. And that's another way you can go
19 through and identify --

20 Q. If something happened?

21 A. If anything happened.

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

♀

59

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

3 A. Yes, it did.

4 Q. And did you --

5 ARBITRATOR CROW: The image was taken on
6 June.

7 THE WITNESS: Fifth.

8 ARBITRATOR CROW: 2005. Okay. Go ahead.

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

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

11-5-10

- 14 Q. Okay. And this modification shows that it was
15 modified on April 29th, 2005. Now, you were
16 here when Mr. Williams explained that he had
17 called Mr. Rote and asked for an explanation.
18 A. Yes, I was.
19 Q. And the explanation was that he had moved the
20 e-mail from one folder to another.
21 A. That's correct.
22 Q. Is that an acceptable explanation for you?
23 A. No.
24 Q. Why not?
25 A. Because even moving a, an e-mail from one area

♀

60

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

17 moved it from this location to old cases. All
18 right. So now even if I moved it from this
19 location in this archive to the next one, it
20 actually does not change the modification date
21 which was the assumption of Mr. Williams when he
22 gave his testimony.

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

♀

61

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

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

8 A. The only way that you can change the last
9 modification date or the only way that the
10 normal users of a computer will change the
11 modification date is by opening up the file and
12 I believe Williams in his testimony said that I
13 can't really modify an e-mail. Well the truth
14 is that within Outlook itself, if you go to
15 edit, you'll see right here, once you've sent
16 it, whether it's sent, whether it's here whether
17 it's in your send mail or drafts, wherever you
18 have this e-mail sitting, if you open it up and
19 go to edit and edit message, then you can

20 change, you can change the body of the e-mail
21 and you can change the subject of the e-mail,
22 et cetera. And once you change it, so if I
23 change it --

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

‡

62

1 A. No.

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

3 A. No, you cannot.

4 ARBITRATOR CROW: Can you change the
5 creation date.

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

12 Q. BY MS. MARSHALL: Okay. So if that's not the
13 answer to why that modification date is
14 April 29th, 2005, did you look into it further
15 to see what the answer is?

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

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

22 A. I did. And, again, as I was explaining with the

23 squares on the wall, there was no activity on
24 the computer from a file metadata perspective.
25 There was no activity on the computer at all on

‡

1 April, April --
2 ARBITRATOR CROW: 29th.
3 THE WITNESS: April 29th, 2005.
4 Q. BY MS. MARSHALL: What does that tell you?
5 A. That tells me that either it wasn't used on that
6 date at all or the information that would tell
7 me has been overwritten because of the time
8 that's passed between when it was actually used
9 and the time I got to examine it.
10 Q. Okay. So if we're looking at the blocks on the
11 wall here, April 29th was a Thursday, as I
12 recall; right?
13 A. Yes.
14 Q. So that block would be blank on the, in what you
15 call the file system?
16 A. Yes.
17 Q. Nothing there at all as if the computer hadn't
18 even been opened?
19 A. That's correct.
20 Q. Okay. Did you go looking for the e-mail, the
21 exit time e-mail?
22 A. Yes, I did.
23 Q. Did you find it?
24 A. On --
25 Q. April 29th.

- 1 A. On which data storage device?
- 2 Q. On the laptop, on Mr. Rote's laptop?
- 3 A. I did find it on the, on Mr. Rote's laptop.
- 4 Q. Okay.
- 5 A. I found the same e-mail that Steve Williams
- 6 found in his report.
- 7 Q. Okay. And I should be referring to when I'm
- 8 talking now, you're using Mr. Williams' forensic
- 9 image and you're using the same forensic tool
- 10 that he was using; is that correct?
- 11 A. Two things. When I originally examined the hard
- 12 drive or the laptop from Rote's, when he gave
- 13 it to me on December 12th of 2008, I was able to
- 14 find the exit time e-mail on his hard drive. I
- 15 was not able to find it at all on any of the two
- 16 drives supplied by or supposedly owned by Max
- 17 Zweizig.
- 18 Q. Okay.
- 19 A. And I was not able to see any activity on the
- 20 four 29 on either my image that was taken in
- 21 2008, December 2008, or on the one provided by
- 22 Zweizig, I mean, sorry, Steve Williams and Mark
- 23 Cox.
- 24 Q. Okay. And have you now found information
- 25 related to the exit time e-mail on April 29th,

- 1 2005?
- 2 A. Repeat that.
- 3 Q. Okay. Well, tell us what you have found with
4 respect to, what happened on April 29th, 2005,
5 with respect to the exit time e-mail?
- 6 A. Nothing that I can find.
- 7 Q. Okay. Did you find more than one version of the
8 exit time e-mail?
- 9 A. No, I haven't.
- 10 Q. All right. Did you find an exit time e-mail in
11 deleted space?
- 12 A. Yes.
- 13 Q. Okay.
- 14 A. Yes.
- 15 Q. Tell us what you found.
- 16 A. So in the image that was provided to me by Mark
17 Cox, which happens to be the image taken by
18 Steve Williams, I found another exit time
19 e-mail, actually we're looking at it right now,
20 another exit time e-mail that was forwarded to,
21 I will put my hand right below it. I found an
22 exit time e-mail the same one that was forwarded
23 to a Ryan Burglhaus, House, not sure how to
24 pronounce it, but that was actually done on
25 which date? On the 29th, 2005. The almost

♀

66

- 1 exact same time as this e-mail was supposedly
2 sent to Max Zweizig or at least not, I'm sorry,

3 that was incorrect. Almost the same exact time
4 as it was stated that this was sent. You know,
5 however, this --

6 Q. Modified?

7 A. Modified.

8 Q. So in the image, and I may have been confusing
9 you because I didn't realize that you were
10 looking at Mr., at the image Mr. Cox had
11 provided you.

12 A. I have not been provided the evidence or images
13 that Steve Williams has really had his hands on
14 or been working on. I only have been provided
15 the, I can't remember what you call it, but the
16 code or the evidence that Mark Cox has been
17 provided.

18 Q. All right. Then I'll refer to that. So in that
19 forensic image you found two copies of the exit
20 time e-mail, one with the metadata that's shown
21 in Mr. Williams' report, the other that had been
22 deleted on April 29th, 2005. Did the one that
23 had been deleted, did it have the same metadata
24 as the one that's shown in the report, create
25 date, delivery date, et cetera?

♀

67

1 A. It only had the same modification date and time.

2 Q. Okay. And did you look at that e-mail to see if
3 it was the same e-mail? Was it an exit time
4 e-mail?

5 A. It was an exit time e-mail. But the created and

11-5-10

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

11 Q. Is that the one you have up there?

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

13 Q. Okay.

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

16 THE WITNESS: Yes.

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

19 THE WITNESS: Correct.

20 ARBITRATOR CROW: Okay.

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

24 A. No.

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

♀

68

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

4 A. Yes.

5 Q. As if nothing it happened?

6 A. Correct.

7 Q. When, in fact, we know something did happen.

8 A. Correct.

9 Q. Now --

10 ARBITRATOR CROW: So you can't tell us what
11 the modification was, if there was a
12 modification, whether it was a change in date or
13 anything of the sort, is that what I'm hearing?

14 THE WITNESS: Yes.

15 ARBITRATOR CROW: So there was a
16 modification but you can't tell us what that
17 modification was.

18 THE WITNESS: That's correct.

19 ARBITRATOR CROW: And there may have been no
20 modification at all, but simply a transfer of
21 the e-mail from one place to another; is that
22 correct?

23 THE WITNESS: That's correct.

24 Q. BY MS. MARSHALL: Well, now wait a minute. That
25 last part, is that really correct, if it was

♀

69

1 just, if the e-mail was just transferred from
2 one folder to another, would that change the
3 modification date? I thought you had testified
4 about that earlier.

5 A. Can you repeat that question?

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

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

11 Q. BY MS. MARSHALL: Well that might be the

11-5-10

- 12 question, too.
- 13 A. Yes. I mean, if, if you simply have changed it
- 14 or moved it, you know, that date will have
- 15 changed.
- 16 ARBITRATOR CROW: Well, as I understand it,
- 17 on April 29th, 2005, this e-mail was sent from
- 18 someone whose name I don't recall or to someone
- 19 whose name I don't recall. Would that create a
- 20 modification date if everything else was the
- 21 same on the e-mail?
- 22 THE WITNESS: Yes.
- 23 Q. BY MS. MARSHALL: Okay. So I don't want to
- 24 confuse it any further.
- 25 A. Okay.

♀

70

- 1 Q. When Mr. Rote said that his explanation being
- 2 that he simply moved the e-mail from one folder
- 3 to another folder, and I thought you testified
- 4 that that did not explain the change, the
- 5 modification date. Have you tested that?
- 6 A. Yes, I have.
- 7 Q. Okay. So now what you're saying is that if it
- 8 were forwarded on that date, that would change
- 9 the modification date?
- 10 A. That's correct.
- 11 Q. Okay. Did you find that it was also deleted on
- 12 that date?
- 13 A. Yes.
- 14 Q. Would that change the modification date?

15 A. I don't know.
16 Q. Fair enough. Because there were two e-mails; is
17 that correct?
18 A. That's correct.
19 Q. Okay. In any case, would it be accurate to say
20 that based on the forensic evidence, something
21 happened to that e-mail on April 29th of 2005,
22 that was different than the explanation that
23 Mr. Rote gave?
24 A. Yes.
25 MS. MARSHALL: Okay. Is it time for a

♀

71

1 break?
2 ARBITRATOR CROW: No. I'm just trying to
3 make sure I understand. If people want a break,
4 we can break.
5 THE WITNESS: I wouldn't mind one.
6 MR. ROTE: I wouldn't mind one.
7 ARBITRATOR CROW: Why don't we take
8 15 minutes then.
9 (Break taken from * to *.)
10 ARBITRATOR CROW: Let's go back on the
11 record.
12 MS. MARSHALL: Are you able to hear okay?
13 MR. ZWEIZIG: Yeah. I did want to is
14 everybody here?
15 MS. MARSHALL: Everybody is here.
16 MR. ZWEIZIG: Whoever got this phone system
17 picked out for me it is great this is a thousand

18 times better than it was before.

19 MS. MARSHALL: Great.

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

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

♀

72

1 is Exhibit 13. Do you have that right there?
2 13 is the termination letter. Were you shown a
3 copy of this letter and asked to perform some
4 forensic examination?

5 A. Yes.

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

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

19 Q. Okay. But I've asked you to do some forensic
20 examination with respect to this letter. And we

21 refer to Exhibit 68, which you say is not in
22 that book?

23 A. No.

24 Q. Okay. It will be in this book here. Exhibit 68
25 is the, as Mr. Williams' report that we were

‡

73

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

3 A. Okay.

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

7 A. Correct.

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

12 A. Yes.

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

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

17 Q. Okay. And who gave it to you?

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

24 and the...

25 Q. Box?

74

1 A. Yeah.

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

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

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

13 Q. And was it marked in any way?

14 A. No, it was not.

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

17 A. No.

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

20 A. Let's see here. Give me a moment. On a floppy
21 disk, this is similar to the floppy disk that I
22 reviewed except for it was green. It was not
23 marked at all. And on a floppy disk there is a
24 tiny switch on the back, this one right here
25 that goes up and down. And that is what sets it

75

- 1 to be either writable or read only where you
2 can't write any data to it.
- 3 Q. When you received it, was the write protect
4 switch on or off?
- 5 A. The write protect switch was off.
- 6 Q. Which means that it could be --
- 7 A. Written to.
- 8 Q. Written to?
- 9 A. Correct.
- 10 Q. And what did you do with the write protect
11 switch?
- 12 A. I turned it to where it was read only so I could
13 not write to it.
- 14 Q. Okay. And then did you create a bit by bit, a
15 bit stream image of the floppy disk?
- 16 A. Yes, I did.
- 17 Q. Was there anyway that you could determine
18 whether this floppy disk was the same floppy
19 disk or the same image that, was it Mr. Williams
20 originally imaged in June of 2005?
- 21 A. Yes. No. No. There was no way to tell.
- 22 Q. Why is that?
- 23 A. Mainly because there's nothing that marks it as
24 original. It's similar to just taking a hard
25 drive out without any sort of identification.

♀

1 There's just no way to tell.

- 2 Q. Okay. Did, can you explain the concept of hash
3 values.
- 4 A. Sure. So a hash value is basically an
5 algorithm. They take every bit of byte that's
6 on this data storage device. It could be huge.
7 It could be like a hard drive. And they perform
8 basically a mathematical equation against every
9 bit or every set of bits on a data storage
10 device. And the hash value at the end is, it
11 becomes the, you know, the original or basically
12 a finger print for whatever the hard drive,
13 whatever that hard drive is. So the hash value
14 in the cases when it comes to forensics is the
15 way to tell if anything is changed on this disk
16 or this drive or this original, you know, data
17 storage device versus, you know, the next one
18 you get or in order to tell that Steve's, when
19 he took the image, the hard drive matches the
20 same image that I took when you performed my
21 data, my forensic imaging.
- 22 Q. Did you have the hash values that were taken
23 when he took his image of the floppy?
- 24 A. No, I did not.
- 25 Q. Okay. But you created, your imaging device

♀

77

- 1 created hash values; is that correct?
- 2 A. Yes. That's correct.
- 3 Q. And did that tell you whether you got a complete
4 copy of the floppy disk?

11-5-10

- 5 A. Yes.
- 6 Q. Okay. Was there anything on the disk other than
7 the termination letter?
- 8 A. Yes.
- 9 Q. Or Max dot --
- 10 A. Maxterm.doc?
- 11 Q. Uh-huh. What else was on that?
- 12 A. There was images, deleted images.
- 13 Q. Images as in pictures?
- 14 A. As in pictures.
- 15 Q. Okay. So it was basically a used floppy disk?
- 16 A. Yes, it was.
- 17 Q. Okay. Do you have your report there so that you
18 can refer to it if you need to?
- 19 A. Mine, yes, I do.
- 20 Q. All right. So after you took a bit by bit image
21 of the floppy disk, did you analyze the image to
22 determine what metadata might help you in
23 determining whether that document was written in
24 October of 2003?
- 25 A. Repeat the question, please.

‡

78

- 1 Q. Okay. Did you analyze or examine the image that
2 you took to determine whether there was metadata
3 that would help you figure out whether the
4 document was, in truth, created October 2nd or
5 October 1st, I guess it is, of 2003?
- 6 A. I mean, I took an image and had my own hash
7 value. But I could not, just having your own

- 8 hash value doesn't tell you that this is
9 necessarily the original or not. It just tells
10 you that whatever your hash value is, you can
11 have that compared to the next person who takes
12 an image of this exact floppy.
- 13 Q. Okay. Let's, I think I'm confusing the issue by
14 referring to hash values. In Mr. Williams'
15 report, which is Exhibit 68, he reports that he
16 found that the dates and times for the creation,
17 create date, modification date and last access
18 date, were October 1st, 2003, at 9:29 a.m.
- 19 A. Okay.
- 20 Q. For two of those. Okay. Did you also look for
21 that kind of metadata in the floppy, on the
22 floppy disk?
- 23 A. No.
- 24 Q. Okay. What did you look for?
- 25 A. I looked to see what data existed on the floppy

♀

79

- 1 disk and verified that there was no corruption
2 on the floppy disk, meaning that the same thing,
3 when you take an image, as I explained to you
4 previously, on the laptop drive, how it reports
5 bad areas, right, the floppy disk does a similar
6 thing. Anything you take does a similar thing.
7 So I can tell whether or not this was, the
8 floppy disk was corrupt in any way.
- 9 Q. Okay. Was the floppy disk corrupt in any way?
- 10 A. No, it wasn't.

- 11 Q. Okay. Did you review Mr. Williams' report with
12 respect to the metadata on the termination
13 document?
14 A. Yes.
15 Q. And do you have that in front of you?
16 A. I don't have his report in front of me, no.
17 Q. Okay. Well, we can get it for you. It's number
18 68. It's right here. It's right here. All
19 right. There it is. Exhibit 68, page three.
20 A. Got it.
21 Q. All right. And at the top he says, the dates
22 and times associated with the document file
23 entry are as follows, create date, October 1st,
24 2003, at 9:29 a.m., modification date,
25 October 1st, 2003, at 9:29 a.m.

♀

80

- 1 Does that in and of itself, is that
2 sufficient to you to verify that that document
3 was, in truth, created on October 1st, 2003?
4 A. No.
5 Q. Why not?
6 A. The reason being is the same reason as before is
7 to prove how easy it is to change your date and
8 time on the computer, well in this case, simply
9 plugging this in having the read only switch off
10 is where I can write to the disk, we'll create
11 the same dates, modified create date modified
12 and last access as I set my date and time to on
13 my computer. So therefore just because it says

14 so on the disk that those are the dates and
15 times, without seeing the original computer that
16 it was actually created on, I'm unable to prove,
17 you know, to the fact that that is exactly when
18 it was really created.

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

21 A. Yes, I did.

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

25 A. Yes, I did.

♀

81

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

3 A. Do we have the printed out one anywhere?

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

6 A. Got it. Okay. I noticed, I'm just going to
7 open it up. I noticed that there was
8 differences in the address, for starters. And
9 unfortunately I don't think I have... . It's
10 tough to tell off of this exhibit without really
11 showing the demonstration on the computer. But
12 there was a difference for the date for
13 starters, this date, the printed out date was
14 ten two instead of 10-1. And it has a full date
15 of 2003 instead of just a two digit date which
16 is '03. The next thing down, this is all off my

17 memory, the NJ for New Jersey, you know, in the
18 original one it was spelled out as New Jersey
19 instead of the two letter abbreviation. And
20 there were some various other names or words in
21 here that were, you know, misspelled or not
22 capitalized or correctly, et cetera, that were
23 also different between the one that was on the
24 floppy disk and the one that was printed out and
25 told that this was what Max Zweizig had

♀

82

- 1 received.
- 2 Q. Okay. So would it be fair to describe
3 Maxterm.doc on the floppy as appearing to be a
4 draft?
- 5 A. Yes.
- 6 Q. Okay. Which, if it were finalized, turned into
7 Exhibit 13; is that right?
- 8 A. That's correct.
- 9 Q. Okay. Based on, just based on the evidence that
10 we've talked about so far, the evidence that you
11 see in Mr. Williams' report, the metadata that
12 shows create date on October 1st and a
13 modification date of October 1st and a last
14 access date of October 1st, and your review of
15 the letter in the forensic file, okay, is there
16 any way that one can conclude that that document
17 was actually finalized on October 2nd, 2003?
- 18 A. The only way to conclude it is if you had the
19 original computer in which the document was

20 created on.
21 Q. Okay. Well, then let's talk about the original
22 computer. How do you know there was an original
23 computer?
24 A. I know that because of the metadata that was
25 found on the floppy disk that was taken, the

‡

83

1 floppy disk image versus the, versus the image
2 that the laptop had. So as an example, I think
3 it's in my report, I have exhibits on here;
4 right? Do we have the exhibits from my report?
5 Q. They should be attached to the report.
6 A. They're not on mine. There's an exhibit that
7 shows a user name, a author, I should say, an
8 author, an author's initials and the company. I
9 don't know where we're going to find it.
10 Q. Does it look like that?
11 ARBITRATOR CROW: We do have --
12 THE WITNESS: Close.
13 Q. BY MS. MARSHALL: Can you work with that?
14 A. This is more of it, yes.
15 Q. Let's use this.
16 ARBITRATOR CROW: What are you looking at?
17 THE WITNESS: This is 185 --
18 MS. MARSHALL: Mark this as Exhibit 185.
19 But I believe it was originally part of his
20 report.
21 ARBITRATOR CROW: Well, show me on the
22 report where it is. What page of the report?

23 I've got arbitration Exhibit 103 and I've got
24 pages eight, nine, ten, 11 --

25 THE WITNESS: This is actually part of my

‡

84

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

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

5 THE WITNESS: This actually isn't mine.
6 Okay.

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

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

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

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

17 Q. What page?

18 A. 12 and 13.

19 ARBITRATOR CROW: Pages 12 and 13?

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

22 ARBITRATOR CROW: All right.

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

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

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

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

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

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

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

4 So what this is showing on 12 and 13, it's
5 simply showing in a very technical, nonlayman's
6 term way of what those equal. So the one that
7 says name user initials and then you'll see, if
8 I can find it, one second, okay. So on 12 and
9 13 in the actual box, the boxes that are right
10 here, these are the actual values that you'll
11 see. So under user initials where it says
12 registry key property value and you'll see R,
13 that's all that was here in this area was here
14 was an R. And then down below you'll see the
15 user name. That's this one where it says name.
16 In this case it says Rote T for I'm assuming Tim
17 Rote. This is coming off of the laptop. And
18 then the next one down below is a company, which
19 is, I don't remember where that is, company is
20 actually here, properties. Company, it simply
21 says NWD. Well that's what the laptop has
22 programmed into it.

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

25 A. Not based on this information. And the reason

♀

87

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

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

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

13 A. Right.

14 Q. So can you tell whether that is accurate?

15 A. Yes.

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

18 A. Yes.

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

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

22 ARBITRATOR CROW: Yeah. I've got 185.

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

25 A. This did.

♀

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

3 A. Okay. So what happens is when you create a Word
4 document and you first save it, like as an
5 example you'll see on the screen here, I have

6 nothing written on this Word document. If I go
 7 to save this document, it's going to ask me to
 8 save it into my documents under the name of
 9 doc1.doc. That's what this first line means on
 10 Exhibit 185 page one. It was actually saved
 11 into and on a hard drive a C drive. The C drive
 12 colon typically means a hard drive somewhere.
 13 So it was saved originally as doc1.doc meaning
 14 it had nothing in it. Because watch on the
 15 screen again if I type anything into this
 16 document like Maxterm, okay, let's say I type
 17 that and then I go hit the save button, then
 18 it's going to try to name my document after the
 19 first thing that I have written into it. So
 20 based on this information that's in Exhibit 185,
 21 it was first saved with nothing in it. Then
 22 what happens --

- 23 Q. BY MS. MARSHALL: Now, where was it saved?
 24 A. It was saved on a C drive, or a hard drive
 25 underneath the user name of owner.

♀

89

- 1 Q. Okay. Now, let's stop there. How do you know
 2 that it was saved --
 3 A. Sorry.
 4 Q. You're kind of fast for me anyway.
 5 A. I am.
 6 Q. How do you know it was initially saved to a hard
 7 drive of a computer?
 8 A. Well, it's an assumption, but based on the

- 9 typical operation of computers and of the
10 Windows operating system, the C drive, C colon
11 backslash is almost always the 1 hard drive on a
12 computer. Right. Take a look at this computer
13 here, okay, the C drive is my hard drive.
14 Q. Okay. And what is typically the floppy drive?
15 A. Typically the floppy drive would be an A drive.
16 Q. Okay. So let's go back to the C drive now. Do
17 we know what hard drive it was that this
18 document was created and saved to?
19 A. No. All we know is that this hard drive, that
20 in that specific location on the hard drive,
21 does not match the laptop.
22 Q. So it wasn't the laptop, but it was a computer.
23 A. Yes.
24 Q. Now, have you read Mr. Rote's testimony about,
25 that he created this document on a computer at

♀

90

- 1 the NDT call center in Eugene?
2 A. Yes, I have.
3 Q. But did not save it to the computer. He saved
4 it to the laptop. So are you saying that that's
5 not exactly accurate? It was saved to a
6 computer?
7 A. That is exactly what I'm saying.
8 Q. Okay. Now, when it was saved to that computer,
9 would the computer, would the hard drive, the
10 operating system on that hard drive create
11 additional metadata that's not on the floppy?

11-5-10

- 12 A. Rephrase, please.
- 13 Q. Okay. Well, let's start with the save, the
14 initial saving, the doc1.doc.
- 15 A. Yes.
- 16 Q. Did doc1.doc have metadata associated with it on
17 the hard drive of that computer?
- 18 A. Absolutely.
- 19 Q. And would that metadata tell you the date and
20 time that the document was created?
- 21 A. Yes, it would have.
- 22 Q. If you had the computer?
- 23 A. If I had the original computer.
- 24 Q. Now, when you work on a document on, even --
25 ARBITRATOR CROW: Unless it was overwritten.

♀

91

- 1 THE WITNESS: Unless it was overwritten.
- 2 ARBITRATOR CROW: All right.
- 3 Q. BY MS. MARSHALL: When you work on a computer
4 using a floppy, does the operating system, the
5 Windows system, capture or save that document in
6 any other way for you?
- 7 A. Yes, it does.
- 8 Q. How is that?
- 9 A. It has what's called an auto recovery. Again,
10 if you don't mind me demonstrating.
- 11 ARBITRATOR CROW: No. No.
- 12 THE WITNESS: If you go again into the
13 options -- they changed it on this one. If you
14 go into the options, you'll notice that it has

15 an auto recover in here. And by default it's
16 set to three minutes, I think if I go, let me
17 exactly show you.

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

21 A. That's correct.

22 Q. And if you do a forensic examination of that
23 computer, are you able to find, assuming it
24 hasn't been overwritten, are you able to find
25 metadata associated with that auto recovery

♀

92

1 file?

2 A. Yes.

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

5 A. Yes.

6 Q. Now, are there other files --

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

8 Q. Go ahead.

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

16 Q. Okay. Are there other files that the
17 original -- Can we call it the originating

- 18 computer now, that the originating computer, are
19 there other files that it will save your
20 document to?
21 A. Yes.
22 Q. And what are those called?
23 A. Those are called temporary files.
24 Q. So this is a third file that the document is
25 created and saved to automatically; is that

♀

93

- 1 right?
2 A. That is correct.
3 Q. All right. On the originating computer. Do the
4 temporary files have metadata associated with
5 them that include date and time?
6 A. Yes, they do.
7 Q. And if you had the original computer, the
8 originating computer and it was not overwritten,
9 would you be able to identify the date and time
10 that that document was created?
11 A. I'd be able to identify the date and time that
12 document was created as well as look at log
13 files to make sure the date and time wasn't
14 manipulated on the original computer.
15 Q. Okay. Were you ever provided the original, the
16 originating computer to examine?
17 A. No, I wasn't.
18 Q. Did you make people aware of the fact that there
19 was a computer out there that had metadata on it
20 you wanted to look at?

11-5-10

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

‡

94

- 1 Q. Is that correct?
- 2 A. Yes.
- 3 Q. Were you ever permitted to examine the
- 4 originating computer?
- 5 A. No, I was not.
- 6 Q. Do you know whether Mr. Williams or Mr. Cox ever
- 7 examined the originating computer?
- 8 A. I do not.
- 9 Q. Without examining the originating computer, can
- 10 you say with any degree of scientific certainty
- 11 whether the metadata on the floppy is accurate?
- 12 A. No, I can't.
- 13 Q. All right. Let's talk a little bit more about
- 14 Exhibit 185 because there's three lines there
- 15 that I need to understand. And I think probably
- 16 Mr. Crow would appreciate an explanation.
- 17 You've talked about the document was
- 18 manually saved by Mr. Rote or whoever the
- 19 operator was once.
- 20 A. Correct.
- 21 Q. And you've talked about the temporary files and
- 22 you have talked about auto recovery. Is there
- 23 metadata here that tells you about the document

24 being saved to a floppy?

25 A. Yes, it does.

95

1 Q. Tell us what that is.

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

15 Now, if you have a look at my screen, I did
16 the same exact order. I saved it as doc1.doc.
17 I will waited until it did an auto save, auto
18 recovery and then I saved it to a floppy disk.
19 And if you look at the disk now you'll see this
20 exclamation mark WRD3744.temp. That is the temp
21 file that I was referring to that is always
22 created wherever you save this document. You'll
23 notice it's the same exact size at the
24 Maxterm.doc. So from a forensics perspective,
25 if the floppy disk that we were given, the green

96

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

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

9 A. That's correct.

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

12 A. Because it does not have metadata that matches
13 the laptop and does not have a temporary file.
14 We cannot see the deleted temporary file even
15 though we can see all the deleted pictures that
16 were on that floppy disk. So it tells me that
17 that was not the original floppy Maxterm.doc was
18 create on.

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

23 A. Yes.

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

♀

1 imaged early on, and if it had been, what would

2 you be able to do with it?

3 A. A few things. I'd be able to match the metadata
4 between the document that was written, that goes
5 with the owner, the user initials and the
6 company. I'd be able to match the metadata and
7 actually find the metadata and the document
8 piece, at least pieces of the document that
9 still existed according to where this says it
10 was saved. I'd be able to term determine if or
11 when that document was originally created, how
12 many times or when it was last accessed, as well
13 as looking at the log files and such in order to
14 determine if the date was ever manipulated. So
15 quite a few things if I had that original
16 computer in front of me.

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

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

‡

1 Q. Okay. Let's go back to the floppy now. In the
2 Exhibit 68, which is I think still over here,
3 Mr. Williams' report where he has the metadata
4 create date and that's October 2nd, 2003, at

5 9:29 a.m. excuse me. October 1st at 9:29 p.m.,
6 or a.m. modification date October 1st, 2003, at
7 9:29 a.m. just as I call the eyeball test, does
8 that suggest to you that this file was simply
9 copied from somewhere else?

10 A. Yes, it does. As Mr. Williams explained earlier
11 during his redirect, just copying files over to
12 a location will, will affect the last, sometimes
13 the, usually what was getting at is it will
14 affect the file created date on any file system
15 that is there. When it comes to a floppy disk,
16 it has a different type of file system than what
17 he was referring to earlier, and, therefore, if
18 you copy a file over to it, the last, the file
19 created data along with the file modified date,
20 the modification date will be exactly the same.
21 So therefore, based on the image that was, that
22 we took that Steve Williams took as well as
23 myself of that, supposedly original green
24 floppy, it wasn't the original, it was a copy of
25 the document onto that floppy disk.

‡

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

11-5-10

- 8 was created?
- 9 A. Yes, exactly how I just explained. It does not
10 contain temporary files. The dates are
11 completely the same on the created and the
12 modified which shows that it was copied over to
13 the disk and not created on it.
- 14 Q. So if the, if the document was not created --
15 Well maybe I should ask you. Was the document,
16 do you have any idea whether the document was
17 created on Mr. Rote's laptop?
- 18 A. No. I mean --
- 19 Q. I asked a bad question. Yeah?
- 20 A. Yeah. Rephrase that, please.
- 21 Q. Was it created on Mr. Rote's laptop?
- 22 A. No.
- 23 Q. And how do you know that?
- 24 A. Because the metadata does not match the laptop,
25 both the metadata does not match the laptop for

♀

100

- 1 the user name, the user initials and the company
2 and the metadata does not match from Exhibit 185
3 of the location. This documents, the settings
4 backslash owner -- I'm slowing down a little bit
5 for you -- the documents and settings, backslash
6 owner is the sign of the windows operating
7 system Microsoft Windows XP home, not
8 professional. So that tells me that whatever
9 computer was utilizing this software had the XP
10 home on it instead of XP professional. The

- 11 I laptop that Mr. Rote provided was XP
12 professional. So that's another indication that
13 this was not created on his laptop.
- 14 Q. Okay. Now, there's another really simple one.
15 The laptop didn't have a slot for a two and a
16 half inch floppy, did it?
- 17 A. From my pictures and my memory, that's correct.
- 18 Q. Okay. So if the floppy disk that you were
19 provided was simply, had simply been copied from
20 somewhere else, okay, how was that copy created?
21 Can you explain how the copy was created?
- 22 A. If it was from somewhere else, meaning not on
23 his laptop, it means that the drive, the
24 computer that he utilized had a floppy disk or
25 he was able to connect one up to it in order to

♀

- 1 copy it from the hard drive where it was located
2 over to the floppy disk.
- 3 Q. Okay. So based on the information we have here,
4 you didn't see the originating computer. You've
5 never seen the original floppy and do we know
6 what computer was used to create the copy of
7 the, that went onto this floppy?
- 8 A. No, we don't.
- 9 Q. And that computer obviously would have metadata
10 in it as well?
- 11 A. Yes, it would.
- 12 Q. Okay. All right. So Mr. Rote testified, you
13 recall reading Mr. Rote testified that he took

11-5-10

14 the floppy home with him with Maxterm.doc on it
15 and either that evening or the next day opened
16 it, changed date and printed it. Okay. Can you
17 tell from the information, the metadata that you
18 were provided, that you got from the floppy,
19 whether that's accurate?

20 A. No. No, you can't.

21 Q. And why is that?

22 A. Because if even printing it as I mentioned
23 earlier, the metadata in the document also saves
24 when it was last printed.

25 Q. Okay. So if we had the original floppy that he

♀

102

1 says he carried home, we would be able to see
2 metadata that would show when it was opened and
3 printed?

4 A. No.

5 Q. Okay. Where do we have to look for the open and
6 printed?

7 A. We have to look on his home PC.

8 Q. So that is now a third computer that may have
9 metadata on it that would show the date and time
10 that this document was created?

11 A. Yes.

12 Q. Did you, were you ever able to examine that
13 computer?

14 A. No.

15 Q. So if we can call that the modifying computer or
16 the second computer, what can metadata would

17 have, would that date, computer have on its hard
18 drive?

19 A. Similar to the originating computer, it would
20 have information about when it was accessed, the
21 date and times of when it was accessed, how many
22 times it was accessed, when it was printed and
23 it would also, it would also contain an auto
24 recovery, depending on how long the document was
25 open for on that computer.

♀

103

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

7 A. My opinion, my opinion is that that was almost
8 as valuable as the original computer that it was
9 created on. Not as valuable only because the
10 original computer should show the original date
11 or have, give someone like me the ability to
12 check the original date when it was actually
13 created versus what we've been told and what was
14 on the floppy disk. That may or may not exist
15 on the secondary computer.

16 Q. Okay. But the secondary computer would tell you
17 when it was printed; correct?

18 A. Yes. Yes, that's correct.

19 Q. Now, I have to ask you not to speculate but I am

11-5-10

20 going to speculate and give you a hypothetical .
21 Okay. Let's say that Mr. Rote, and fed a peek
22 or whatever on October 1st thought about firing
23 Mr. Zweizig, sat down and drafted the letter and
24 then thought better of it and didn't, didn't
25 send it. Okay. The metadata that we see in

♀

104

1 Mr. William's report that you have described
2 would all be there, it was created on
3 October 1st?
4 A. That's correct.
5 Q. Okay. But you can't tell whether it was printed
6 on October 2nd without the second computer, can
7 you?
8 A. That's correct as well.
9 Q. Is it possible that even though it was created
10 on October 1st, it could have been printed on
11 October 30th after maybe other incidents have
12 happened?
13 A. Without having the computers around that it was
14 printed on, there's no way to tell. So it's
15 possible, absolutely possible.
16 Q. So am I accurate in concluding that the metadata
17 in Mr. Williams' report describes a draft and
18 nothing more?
19 A. Possibly.
20 Q. Okay. Well, I asked Mr. Williams whether it was
21 possible, whether three scenarios are possible,
22 one is that one could reset the clock and type

11-5-10

23 the letter up any time you want and it would
24 show that metadata. If you told the computer it
25 was October 1st, that's what the computer would

‡

105

1 think. The second is that you could draft the
2 letter on October 1st, think better of it,
3 change your mind, whatever, and then after
4 incidents later in the month, decide, by golly,
5 I am going to fire him. So then you finalize
6 the document and print it. That's possible
7 given the metadata that we have, isn't it?

8 A. Yes.

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

13 A. That's correct.

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

21 A. That's correct.

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

25 A. December 12, 2008.

- 1 Q. Okay. Same time that you got the floppy and
2 examined Mr. Rote's laptop?
- 3 A. That's correct.
- 4 Q. And was the 60-gigabyte installed in the
5 computer?
- 6 A. Yes, it was.
- 7 Q. So you were able to match it up and tell that
8 that actually ran on that computer; right?
- 9 A. Yes. Yes.
- 10 Q. And did you make a forensic image of the
11 60-gigabyte hard drive?
- 12 A. Yes, I did.
- 13 Q. And the same way that Mr. Williams described
14 that he had made a forensic image?
- 15 A. Correct.
- 16 Q. And did you examine that, well let me ask you,
17 what were the issues that you were asked to
18 examine that 60-gigabyte hard drive for?
- 19 A. I was asked to actually examine the 60-gigabyte
20 hard drive, the laptop drive as well as 120
21 gigabyte hard drive for any, any relevant
22 documents dealing with Max's termination in the
23 year 2003. That's the first thing I was asked
24 by the stipulation order.
- 25 The second thing I was asked was to review

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

5 ARBITRATOR CROW: On which computers.

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

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

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

♀

1 the year of 2003. I was not specifically
2 looking for e-mails and I was not specifically

- 3 Looking for the exit time e-mail.
- 4 Q. Okay. So you're looking generally for anything
- 5 having to do with the termination. Did you find
- 6 anything?
- 7 A. Yes, I did.
- 8 Q. What did you find?
- 9 A. I found the exit time e-mail as an example. I'm
- 10 sorry. Not on the 60-gig. I found nothing.
- 11 ARBITRATOR CROW: Nothing on the 60.
- 12 THE WITNESS: I found absolutely nothing on
- 13 the 60-gig Drive. Excuse me.
- 14 Q. BY MS. MARSHALL: Okay. You know that Mr. Cox
- 15 did an examination of the 60 either in 2009 or
- 16 2010. And also found no e-mail traffic on the
- 17 60.
- 18 A. I am aware.
- 19 Q. Did you, did you review Mr. Williams' report to
- 20 see whether he found any evidence of e-mails on
- 21 the 60?
- 22 A. Yes, I did.
- 23 Q. This is back in 2005. And he found a series of
- 24 e-mails, did he not?
- 25 A. That is correct.

♀

109

- 1 Q. Okay. And I want to draw your attention to one
- 2 of them, in particular. This is Exhibit 71.
- 3 You will find it over here. 71. Okay. Page
- 4 eight.
- 5 ARBITRATOR CROW: Page eight.

- 6 Q. BY MS. MARSHALL: Yes. I'm sorry. I should
7 have let you --
- 8 A. No problem. Okay.
- 9 Q. Now page eight number five. Now there's been
10 some testimony about, that these e-mails were
11 just parts of e-mails that were sent to somebody
12 else. Number five here, in Mr. Williams'
13 report, is printed off of the Sony Vaio in 2005.
14 Well, tell us what that file, that line of file
15 information tells us?
- 16 A. That path?
- 17 Q. Yes. File path?
- 18 A. That file path indicates that it's an Outlook
19 storage file for all e-mail coming into Outlook
20 and that it belongs to the account Jay Ci offi,
21 which I believe was owned by Joe Ci offi from
22 NorthWest Direct.
- 23 Q. Okay. And it's an Outlook PST file?
- 24 A. That's correct and it is not deleted.
- 25 Q. And it's not in deleted space?

♀

110

- 1 A. No.
- 2 Q. Okay. And it says original message from Irene a
3 somebody, *Ranoff, to Brent *Cowiak and
4 Max@NWtel emarketing. com.
- 5 A. Correct.
- 6 Q. Do you see that? Now, would that indicate to
7 you that at some point in time prior to at least
8 2005, that computer had been used to receive

- 9 that original message?
- 10 A. Yes.
- 11 Q. Okay. Did you see that message when you went
12 looking for e-mails in 2008?
- 13 A. No.
- 14 Q. Do you have any idea why?
- 15 A. Two reasons. One, it did not match the search
16 terms that I am put in for termination for Max
17 termination, and second, it could have been
18 deleted years later and I would not have been
19 able to find it.
- 20 Q. But Mr. Cox couldn't find it either and he was,
21 he did testify that he was looking for that,
22 that e-mail address?
- 23 A. That's correct.
- 24 Q. Okay. So, in your judgment what would explain
25 why Mr. Williams would find it in 2005 and

♀

111

- 1 Mr. Cox would not find it in 2009 or 2010?
- 2 A. The latter of my previous explanation. It means
3 it was deleted and overwritten by the time that
4 Mr. Cox was doing his search. And I should add
5 onto that, just because he didn't find it could
6 mean that just the very top portion with Max's
7 e-mail part was deleted, not necessarily the
8 entire e-mail. But he wouldn't have hit on the
9 rest of this e-mail without, because he was
10 searching for Max only.
- 11 Q. I'm not sure I follow you.

- 12 A. Okay. So in forensics we use keywords to do our
13 searches across the entire data storage device.
14 Right. And in Mr. Cox's case my assumption is
15 that he searched for Max@NWtelmarketing or he
16 just searched for Max, just as an example.
17 Well, if, if part of this file got wiped out
18 like that original message and down four lines,
19 that got wiped out but the rest this have still
20 existed, he would not have found it because
21 nothing else in this message matches Max or
22 Max@NWtelmarketing.com. So it's possible that
23 this still exists on the hard drive, just not
24 the portion that is on the very top.
25 Q. Okay. So in your judgment would you say that

♀

112

- 1 the conclusion that the 60-gigabyte hard drive
2 was never, most certainly never used to receive
3 e-mails or reach?
4 A. I don't agree with that. So it was used,
5 definitely used for e-mail at one point in time.
6 MS. MARSHALL: All right. If it would be
7 okay, it's straight up 12:00. And.
8 ARBITRATOR CROW: That's fine for a break.
9 MS. MARSHALL: It would be.
10 ARBITRATOR CROW: If you would like to do
11 that.
12 MS. MARSHALL: I would.
13 ARBITRATOR CROW: All right. We'll go off
14 the record.

11-5-10

(Break taken from * to *.)

15

16

ARBITRATOR CROW: All right. Go ahead.

17

Q. BY MS. MARSHALL: I want to, I may have confused

18

an issue this morning in the way I asked a

19

question. And so I just want to make sure that

20

Mr. McAnn has an opportunity to clarify. And

21

it's just a very simple question relating to the

22

exit time e-mail. When you move an e-mail from

23

one folder to another, does it change the last

24

modified date?

25

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

♀

113

1

ARBITRATOR CROW: All right.

2

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

3

A. I am absolutely certain of that.

4

Q. All right. Let's finish up talking about the

5

60-gigabyte hard drive that you examined. I

6

believe you said that you were instructed, first

7

of all, to look for anything related to

8

Mr. Zweizig's termination.

9

A. Yes.

10

Q. And the other issue that you were asked to look

11

for was extra job kinds of activities like porn.

12

A. That's correct.

13

Q. All right. Did you examine the 60-gigabyte hard

14

drive, the image of the 60-gigabyte hard drive

15

for porn?

16

A. Yes, I did.

17

Q. Okay. And did you find any?

11-5-10

- 18 A. No, I did not.
- 19 Q. Did you find an image or any images on the
- 20 60-gigabyte hard drive that could be considered
- 21 to be porn?
- 22 A. No, I did not find any images at all. The only
- 23 thing that I found similar to Mr. Cox, is, and
- 24 maybe even Steve Williams, if I remember right,
- 25 is file names that represent or could be

♀

114

- 1 pornography. However, all of the file names
- 2 and --
- 3 Q. Okay. Before you go any further, I'm still
- 4 talking about the 60-gigabyte not the
- 5 120-gigabyte?
- 6 A. My fault. Sorry.
- 7 Q. It might have been mine. Just sticking with the
- 8 60-gigabyte hard drive for the moment, did you
- 9 search it for anything that might be porn?
- 10 A. Yes.
- 11 Q. Okay. And what did you find?
- 12 A. I didn't find anything that related to porn at
- 13 all in the 60-gigabyte hard drive.
- 14 Q. Okay. Now, do you have experience that would
- 15 permit you to examine with some authority
- 16 looking for porn?
- 17 A. Yes. During my time working for different
- 18 corporations, that goes for AT&T wireless for
- 19 nine years as well as *PACR for two years, a lot
- 20 of their cases are considered policy violations.

21 So most of the cases that I do on a corporate
22 level are pornography cases. That's hundred,
23 I've done at least 100 pornography cases.

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

‡

115

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

8 Q. Okay. And in this case did you do that with the
9 60-gigabyte?

10 A. Yes, I did.

11 Q. And what did you find?

12 A. I did not find any pornography.

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

15 A. No, I did not. Not on the 60-gigabyte hard
16 drive.

17 Q. Okay. I just want to make --

18 A. I'm sorry.

19 Q. Make sure we are you can talking about the same
20 hard drive I am thinking about and the same
21 images I am thinking about.

22 A. I'm sorry. Must be the lunch I did, I found
23 three, three images that could be considered

24 pornographi c.

25 ARBITRATOR CROW: On the 60-gi gabyte.

116

1 THE WITNESS: On the 60-gi gabyte hard drive.

2 Q. BY MS. MARSHALL: Okay. And without getting
3 into too much detail can you tell us what those
4 three are?

5 A. There were two images of male genitalia and one
6 image of a woman's breast.

7 Q. And in terms of --

8 ARBITRATOR CROW: That's on the image, not
9 on a hard drive? Am I correct?

10 THE WITNESS: No. Those are images that are
11 on the 60-gi gabyte hard drive.

12 ARBITRATOR CROW: Oh. I understood you to
13 say earlier that you found no pornographi c
14 reference on the 60-gi gabyte hard drive.

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

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

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

21 ARBITRATOR CROW: All right.

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

117

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

4 A. I can tell you that one of the pictures
5 occurred, well, had a date and time stamp of
6 September, I believe, 2003. Yep.
7 September 30th, 2003. The other two images did
8 not, and unfortunately without my exhibits I
9 can't tell you when they were, but they, the
10 other two, one of the male genitalia and one of
11 the woman's breast actually belonged to the
12 account named Jay Ci offi. So Joe Ci offi's
13 account.

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

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

20 ARBITRATOR CROW: On the 9-30?

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

♀

1 that's actually on page, that's on Exhibit 103,

2 page 11, where the Jay Cioffi account accessed
3 that image once in December of '04 and again in
4 July of '08.

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

9 THE WITNESS: November, I believe of 2003.

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

14 THE WITNESS: It wasn't actually accessed on
15 9-30-03. That's simply the date and time like
16 the creation date and time stamp as well as the
17 last written date and time stamp. There's a,
18 there's a difference between looking for
19 activity and activity showing that somebody
20 actually went to that picture and touched it
21 versus a date that says it was touched by
22 something. An example, if you look again on
23 page 11 of example, of Exhibit 103, you'll see
24 last access date. And those could be caused by
25 anything. They could be your anti virus

♀

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

3 ARBITRATOR CROW: Okay. I'm not sure but
4 what we're off on a side bit of testimony here,

5 I don't recall having seen or heard any
6 testimony that would suggest NorthWest Direct
7 tell services had a policy which would prevent
8 an employee from accessing whatever he or she
9 wanted to during particularly during nonworking
10 hours. Has there been any such testimony?

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

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

18 MS. MARSHALL: That's right.

19 ARBITRATOR CROW: All right.

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

22 A. That's correct.

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

‡

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

3 A. Correct.

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

6 A. Again, I specialize in incident response, which
7 comes to computer compromises. So I have a lot

8 of experience when it comes to utilizing
9 applications to delete data, hide data,
10 et cetera.

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

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

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

♀

121

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

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

6 A. The software would be there to encrypted data
7 such as private data for either their company or
8 other companies in order to protect it from
9 being compromised.

10 Q. When it was sent from client to --

- 11 A. Exactly.
- 12 Q. -- et cetera, back and forth. Okay. What would
- 13 be the signature that you would see if it were
- 14 used to actually wipe something off of the
- 15 60-gigabyte?
- 16 A. It would do a, it would do 255 characters
- 17 because that's the maximum length you can have
- 18 for a file name of like all A's or all B's or
- 19 all something like that. And it would do that
- 20 whether it's a file or a folder.
- 21 Q. And you didn't find any of those?
- 22 A. I did not find that.
- 23 Q. All right. Did you find any evidence that any
- 24 Fox Pro files had been deleted?
- 25 A. I did find Fox Pro files on there that were

♀

122

- 1 deleted but they were deleted after the date,
- 2 after the 2003 date that Max Zweizig was,
- 3 supposedly had that computer in his possession.
- 4 ARBITRATOR CROW: Wait just a moment.
- 5 Q. BY MS. MARSHALL: Okay. Let's move on to --
- 6 ARBITRATOR CROW: Wait a minute.
- 7 (Record read. *
- 8 ARBITRATOR CROW: Could you do you mean
- 9 after it was no longer in his possession?
- 10 THE WITNESS: After 11-13-2003.
- 11 ARBITRATOR CROW: Okay. That was my
- 12 confusion. Go ahead.
- 13 Q. BY MS. MARSHALL: Let's go on to the

14 120-gigabyte hard drive. I want to talk about
15 your examination of the hard drive. When you
16 went to Mr. Rote's attorney's office in December
17 of 2008, were you provided the hard drive at
18 that time?

19 A. No. Well --

20 Q. What were you given?

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

24 Q. What was in the CD rom?

25 A. A CD rom.

♀

123

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

3 A. No, it's not.

4 Q. So what did you do?

5 A. I told, actually Mr. Edelson was not there. So
6 I told Mr. Edelson's assistant that it did not
7 contain the 120-gigabyte hard drive --

8 ARBITRATOR CROW: I can hear you.

9 THE WITNESS: I'm sorry.

10 ARBITRATOR CROW: Don't worry. I'm not a
11 jury.

12 THE WITNESS: So I explained that they, that
13 it did not contain 120-gigabyte hard drive.
14 So they contacted Edelson, who contacted
15 somebody else and I believe they may have
16 contacted Mr. Rote at that time and said that

17 they must have replaced or misplaced it and that
18 I would have to come back at a later time.

19 Q. Okay. So then did you make another trip back
20 here from Seattle to, at another, at a later
21 date?

22 A. I did. So that was in December of '08 that I
23 came back and sorry I was moving around. I am
24 just going to go pull up my invoice so I can
25 remember the date in February but it's probably

♀

124

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

5 ARBITRATOR CROW: February 2008.

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

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

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

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

17 A. Well, again I was under the assumption that they
18 had found the hard drive. And in this case Tim
19 Rote was there and the, they presented me or

20 provided me a external drive that contained an
21 image of the supposed hard drive on there. So I
22 contacted at the time James Dow, who was the
23 attorney for Max Zweizig, and they just said,
24 well they couldn't find the hard drive, the
25 original hard drive, but Steve Williams was able

‡

125

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

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

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

9 ARBITRATOR CROW: I understand.

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

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

19 ARBITRATOR CROW: Did you ever examine the
20 120 gigabyte hard drive.

21 THE WITNESS: Yes, I did.

22 Q. BY MS. MARSHALL: Well, the question is did you

23 ever examine the hard drive?

24 A. No.

25 ARBITRATOR CROW: Okay. You just had an

126

1 image of an image.

2 THE WITNESS: (No audible response.)

3 ARBITRATOR CROW: All right. Thank you.

4 THE WITNESS: Sorry. Yes.

5 Q. BY MS. MARSHALL: So what does this, as a
6 forensic examiner, what does this tell you about
7 the litigation hold with respect to the
8 120-gigabyte hard drive?

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

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

18 A. No.

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

21 A. No.

22 Q. Okay?

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

25 ARBITRATOR CROW: Tim, before you ask any

1 questions, let me understand --

2 MR. ROTE: Sure.

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

8 THE WITNESS: That's correct.

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

12 THE WITNESS: Yes, I did.

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

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

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

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

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

24 ARBITRATOR CROW: We're talking about the
25 120-gigabyte image of an image; is that correct?

1 That's what you had to examine?

2 THE WITNESS: Yes.

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

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

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

13 THE WITNESS: Oh.

14 ARBITRATOR CROW: Go ahead.

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

22 ARBITRATOR CROW: To your report?

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

♀

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

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

5 THE WITNESS: 103.

6 ARBITRATOR CROW: -- 103. Yeah.

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

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

13 THE WITNESS: Right. I do not see --

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

18 THE WITNESS: It appears so, yes.

19 ARBITRATOR CROW: All right.

20 MS. MARSHALL: If it's okay, we can, we can
21 make sure that that exhibit is complete. It
22 doesn't appear that it is at the moment.

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

♀

130

1 MS. MARSHALL: Okay.

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

6 terminated?

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

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

18 THE WITNESS: Yes, sir.

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

♀

131

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

8 I also would like to have from you,

9 Mr. Rote, a reference to anything that is in the
10 record about advice to you of the need for a
11 litigation hold. You now understand what a
12 litigation hold is, I assume.

13 MR. ROTE: Yes, I do.

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

18 MR. ROTE: Okay.

19 ARBITRATOR CROW: Okay. Cross-examination.

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

♀

132

1 reformatted on November 12th, 2003.

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

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

6 ARBITRATOR CROW: On Exhibit 103 you are
7 talking about.

8 MR. ROTE: On Exhibit 103. I had separate
9 records but I had only exhibits one through
10 eight. Only a few exhibits are attached as part
11 of this report. So we're still kind of back to

12 some of the exhibits in your original report
13 never made it into the record.

14 THE WITNESS: Okay.

15 Q. BY MR. ROTE: But let's go on with respect to
16 the question which was that you concluded that
17 the 120-gigabyte hard drive had been reformatted
18 on November 12, 2003?

19 A. That's correct.

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

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

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

♀

133

1 NWD identifications, do you recall?

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

4 Q. Yes, I am.

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

7 Q. So they were all Fox Pro files?

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

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

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

11-5-10

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

20 Q. Did you find a reformat date before December 12,
21 2000, -- I mean, November 12, 2003?

22 A. No.

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

25 A. No.

♀

134

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

4 A. Did I put that in my report?

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

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

9 Q. You didn't find any pictures?

10 A. Right.

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

12 A. No. All the video files that were named in a
13 fashion that would line up with pornography I
14 was unable to recover.

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

11-5-10

- 18 A. I was able to determine that.
- 19 Q. Okay. Did, were you able to determine that
- 20 there was a substantial amount of activity with
- 21 respect to that?
- 22 A. Yes, I was.
- 23 Q. Okay. And the dates and times for many of those
- 24 files were during the course of the period of
- 25 time from May 2003 until it was reformatted in

♀

135

- 1 November 2003?
- 2 A. Yes.
- 3 Q. That's correct? That's a period of time in
- 4 which Mr. Zweizig testified that it was in his
- 5 fireproof safe. You found dates and times for
- 6 files during that period of time?
- 7 A. Yes.
- 8 Q. Okay. With respect to the 60-gigabyte hard
- 9 drive, you had mentioned that, I want to focus
- 10 on e-mail activity right now. I think your
- 11 testimony was there was evidence that the
- 12 60-gigabyte hard drive had been used for e-mail?
- 13 A. Yes.
- 14 Q. But the question is was it used by Mr. Zweizig
- 15 for e-mail. Has it been used by Mr. Zweizig for
- 16 e-mail?
- 17 A. Not that I found.
- 18 Q. Not that you found. So the question itself kind
- 19 of missed the mark on that. The real question
- 20 is was it used by Mr. Zweizig for his e-mail?

11-5-10

- 21 The answer is no?
- 22 A. No. Not that I found.
- 23 Q. Not that you found. Okay. When you're
- 24 examining log files for change dates, et cetera,
- 25 you must have found some change dates in the log

‡

136

- 1 files that you did find. What, for the, for the
- 2 laptop that you examined, for the exit time
- 3 e-mail, did you find any changed dates at all?
- 4 A. Actually I didn't find any changed dates at all
- 5 on any of the files on any of the --
- 6 Q. For any of the computers?
- 7 A. For any of the computers.
- 8 Q. Let me ask you about the credibility of forensic
- 9 scans. You had mentioned that you didn't get
- 10 the 120-gigabyte hard drive. You only received
- 11 a forensic scan.
- 12 A. A forensics image.
- 13 Q. Forensic image. I'm sorry. Do you find that
- 14 having a forensic image is not the same as
- 15 having a hard drive?
- 16 A. Absolutely.
- 17 Q. You do believe that?
- 18 A. Yes.
- 19 Q. And the forensic, I think Mr. Cox testified that
- 20 he typically travels around the country and does
- 21 forensic work and it's less common for him to
- 22 actually pick up hard drives. He takes forensic
- 23 scans, forensic images and uses those as his

24 tool?

25 A. I must have missed that in his testimony because

137

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

6 Q. Okay. But the question then with respect to a
7 copy of a forensic image, would you say that a
8 copy deteriorates that forensic image, is that
9 your position?

10 A. Yes. It comes down to best evidence. In some
11 cases you will be limited to a copy, an image,
12 not the original. Right. But the original is
13 what every practiced forensic examiner should be
14 going for.

15 Q. And with respect to the 120-gigabyte hard drive,
16 that's all you have was the forensic image?

17 A. That's correct.

18 Q. But you found no activity of use after
19 November 12th of 2003; is that correct?

20 A. That's correct.

21 Q. After it was reformatted, there was no evidence
22 of activity?

23 A. Correct.

24 Q. Okay. Now, on the 60-gigabyte hard drive, that
25 continued to be in use. So that was scanned,

138

- 1 forensic image was made I believe May 2005. And
2 continued to be in use thereafter. You did a
3 forensic, your own forensic image?
4 A. It was June 2005. And yes.
5 Q. You did your own forensic image subsequent to
6 that date but you also had Mr. Williams'
7 forensic image on that date for the June 2005?
8 A. You say subsequent.
9 Q. Well you received a copy of his forensic image
10 or received a forensic image?
11 A. Last weeks.
12 Q. That he provided?
13 A. Steve Williams?
14 Q. Steve Williams, well, the chain was Steve
15 Williams provided it had to Mr. Cox and Mr. Cox
16 provided it to you.
17 A. Okay. In that case I have received a copy of
18 the 60-gigabyte hard drive from Steve Williams.
19 My understanding is it was from Mr. Cox.
20 Q. Okay. So Steve Williams provided that forensic
21 image which he took in June 2005 to Mr. Cox.
22 Mr. Cox provided a copy of that to you. Okay.
23 And that, and you evaluated that 60-gigabyte
24 hard drive image as of June 2005?
25 A. Correct.

♀

- 1 Q. And so your basis then was that in thinking back

- 2 now to the volume of e-mail activity, you again
3 to reiterate found no evidence that Mr. Zweizig
4 used --
- 5 A. I did -- I'm sorry to interrupt.
- 6 Q. That's okay.
- 7 A. I did not do any searches for e-mail other than
8 the exit time e-mail on the 60-gigabyte hard
9 drive.
- 10 Q. You did not do any additional work to evaluate
11 whether or not that, there was a volume of
12 activity with respect to the 60-gigabyte hard
13 drive?
- 14 A. No. Not on the one provided to me that was
15 provided to me by Mark Cox from Steve Williams.
- 16 Q. I see. But you did on your first, on your
17 forensic image?
- 18 A. Yes.
- 19 Q. And you found no evidence of use by Max Zweizig?
- 20 A. No.
- 21 Q. Okay. What was the, you found no use by
22 Mr. Zweizig?
- 23 A. On the 60-gigabyte hard drive.
- 24 Q. On the 60-gigabyte hard drive. Now, on the
25 120-gigabyte hard drive, did you examine that

‡

140

- 1 for e-mail activity for Mr. Zweizig?
- 2 A. Yes, I did.
- 3 Q. And did you find a lot of e-mail? Did you find
4 evidence of use?

- 5 A. I did find e-mail and evidence of use.
- 6 Q. And it was substantial?
- 7 A. I found two what they would call PST files. So
- 8 storage for e-mail and they were quite large.
- 9 However, they were also corrupt so I couldn't
- 10 get every e-mail out of them.
- 11 Q. But you did find substantial --
- 12 A. I did.
- 13 Q. -- e-mail. And you would have expected to find
- 14 substantial volumes of e-mail?
- 15 A. Yes.
- 16 Q. Okay. With respect to the floppy drive, you had
- 17 indicated that on Steve Williams' report,
- 18 Exhibit 71, page five, I believe, that, if you
- 19 can turn to that, please.
- 20 A. I got it. No.
- 21 Q. Let's see. Exhibit 71. Maybe it's exhibit 60.
- 22 Let me go there. Exhibit 68, arbitration
- 23 Exhibit 68, page three, if you could go there,
- 24 please. You had indicated that the date and
- 25 time stamps for create date and modification

♀

- 1 date, you reached a certain conclusion about
- 2 that. Would you restate that conclusion?
- 3 A. The conclusion is that they are the exact same,
- 4 so therefore it was copied, that Maxterm.doc was
- 5 copied to the floppy drive not created on it
- 6 originally.
- 7 Q. So it could have been, could have been drafted

- 8 on this other computer and saved only one time
9 and it would create the same statement, is that
10 the same conclusion?
- 11 A. The conclusion is it was drafted on some other
12 computer or a computer, saved somewhere. Now
13 according to the, according to the document that
14 was saved on that floppy disk, I haven't say
15 saved, that was examined on that floppy disk, it
16 was saved not only to a hard drive but to a
17 floppy disk at some point in time. Just not
18 that floppy disk that I received.
- 19 Q. You're maintaining that because these two dates
20 are the same, you reached a conclusion and the
21 times are the same -- Are the times on there?
22 They are. That that represents a copy?
- 23 A. That and because it didn't contain the temp
24 files that go along with creating or saving a
25 file to a document to a floppy disk.

♀

142

- 1 Q. So, but isn't your position that if that
2 document was created on a computer that had a
3 floppy drive and a hard drive, C drive, that if
4 Microsoft Office was just brought up and that
5 document was created, wouldn't the temp file
6 have been on the C drive?
- 7 A. Both.
- 8 Q. It would be in both places.
- 9 A. Yes.
- 10 Q. So the temp file then, the metadata with respect

- 11 to the temp file, wouldn't have been copied over
12 to that other floppy? Is that the point?
- 13 A. No. Not the point. The temp file would not
14 have been copied over to the other floppy disk.
- 15 Q. I see. Okay. With respect to the 60-gigabyte
16 hard drive and the identification of the Fox Pro
17 files you were asked to search for deleted files
18 and you found a substantial number of deleted
19 files after Mr. Zweizig turned over the
20 computer. Do you recall the dates?
- 21 A. Yes. Well, I recall that it was December, I
22 believe 29th of '03 and above.
- 23 Q. And after?
- 24 A. And after.
- 25 Q. Were you asked to look for the existence of Fox

♀

143

- 1 Pro files that had date stamps prior to
2 November 13, 2003?
- 3 A. I was asked -- No, not specifically.
- 4 Q. So you were only asked to look for deleted
5 files, not Fox Pro files that were created prior
6 to November 13, 2003?
- 7 A. That is correct. But I am verifying with the
8 stipulation order. That is correct. The only,
9 the only restriction or limit that I had for the
10 year 2003 was the examination of media for the
11 limited purposes of identifying records from
12 2003 relating to the creation, modifying,
13 editing, storing, chain of custody, receipt and

14 transmission of the termination letter or
15 derivations thereof. So the actual look for
16 destroy and tampered with files was not limited
17 to 2003.

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

20 A. Personal computers?

21 Q. Personal computers.

22 A. No.

23 Q. Laptop. He had a laptop?

24 A. No.

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

♀

144

1 A. No.

2 Q. And your conclusion with respect to the exit
3 time on the e-mail was that, was that the dates
4 and times associated with that e-mail are
5 accurate?

6 A. Accurate in the sense that they were definitely
7 sent at that date and time would be no. If you
8 mean that the computer was accurate when it put
9 on those date and times based on whatever the
10 computer time was? I would say yes.

11 Q. Your testimony is that you have not been able to
12 refute that evidence; is that correct?

13 A. That's correct.

14 Q. And not that it didn't happen, just that you
15 weren't able to refute it?

16 A. I don't have any collaborating evidence that

17 tells me one way or another if it's accurate or
18 not.

19 MR. ROTE: Okay. That's all. Thank you.

20 ARBITRATOR CROW: Redirect.

21 Q. BY MS. MARSHALL: Yes. I just want to make sure
22 that I understand correctly. When Mr. Rote drew
23 the distinction between the e-mail that you
24 testified about that, if you recall that was an
25 original message that was from someone else to

♀

145

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

7 A. Yes.

8 Q. Is that it?

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

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

16 Q. Okay. Tell me what's correct.

17 A. And the reason being you cannot distinctly say
18 that number five on his report was to Max on
19 that computer or Brent or Bret or any of the

20 other people that were on that computer, in that
21 original e-mail. So therefore, you can't say
22 that he was receiving on that computer. And the
23 same thing goes for sent. Now, I am going based
24 on, I would be going based on sent from him.
25 However, even at that point there has to be a

‡

146

1 direct file at that really tells you that it
2 was, that it belonged to him. You cannot make
3 the assumption that either or is delivery or
4 activity by Mr. Zweizig.
5 Q. Okay. But in any case by 2008 you couldn't find
6 that e-mail?
7 A. No.
8 Q. You were asked in cross whether you found that
9 the 120-gigabyte had been reformatted prior to
10 November of 2003 or prior to the November 12th
11 date. And I believe you testified that you
12 would not expect to find that. Why not?
13 A. Only because it's, it's, I don't know. It's not
14 a usual thing to reformat the drive over and
15 over again. Now, there are ways to check and
16 see previous formats, but I did not run through
17 that type of examination.
18 Q. Okay. But you didn't see any evidence that
19 it --
20 A. No.
21 Q. -- had or had not been -- Okay.
22 A. You skipped a page.

- 23 Q. Pardon?
24 A. You skipped a page.
25 Q. I'm sorry. You're anticipating my questions?

‡

147

1 MS. MARSHALL: I have no other questions.

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

5 MS. MARSHALL: Yes, we do.

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

8 MR. ROTE: One witness.

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

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

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

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

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

22 (Break taken from * to *.)

23 ARBITRATOR CROW: Let's go back on the
24 record then. And Mr. Rote, as I understand it,
25 wants to provide some additional testimony in

1 his case in chief.

2 MS. MARSHALL: Mr. Zweizig, what's happening
3 is that the next witness is not available until
4 2:30 and Mr. Rote has some testimony that he
5 wants to put on the record and I have a question
6 or two that I want to ask him. So that we're
7 going to do that right now. That's why we
8 called you back.

9 MR. ZWEIZIG: Okay. Thank you. I'll just
10 be here.

11 ARBITRATOR CROW: As I understand it,
12 Mr. Rote, do you want to reopen your case in
13 chief and provide some additional evidence; is
14 that correct.

15 MR. ROTE: I do.

16 ARBITRATOR CROW: All right. Proceed.
17 You're already under oath.

18 MR. ROTE: Yes. Exhibit 149, I wasn't sure
19 that the record was clear enough about the
20 history of demand for compensation and request
21 for mediation as well as our response to that.
22 And so I have included in Exhibit 149 the
23 history, both in terms of the demand from
24 Zweizig's counsel in New Jersey, John Wiles'
25 response to that demand, the arbitration

1 service, arbitration service of Portland
2 agreement to mediate, additional correspondence
3 to Kevin Costello with respect to that matter.
4 Starting on page then the communication with the
5 mediator in New Jersey with respect to the
6 matters, our mediation statement with respect to
7 all of that data. So the only thing that I
8 wanted to get in the record was that history
9 since that question has been challenged with
10 respect to our additional claim, I wanted to
11 make sure that we had that history covered.

12 ARBITRATOR CROW: All right.

13 MS. MARSHALL: The only thing that I would
14 object to here is the mediation statement. If
15 I'm not mistaken, Oregon law prohibits the
16 introduction into evidence under any
17 circumstance of communications during mediation.

18 ARBITRATOR CROW: And that is, what part of
19 the exhibit is that?

20 MS. MARSHALL: That starts on page 11.

21 MR. ROTE: Yeah. It does.

22 MS. MARSHALL: That's what I'm always told
23 by mediators anyway.

24 MR. ROTE: 11, 12, 13 and 14 and 15 and 16,
25 17 --

♀

150

1 ARBITRATOR CROW: I think Ms. Marshall is
2 correct in that respect. What is your response?

3 MR. ROTE: I'm fine with that. We can
4 remove page 11 back.

5 ARBITRATOR CROW: Take them back and I won't
6 bother with them. Okay. Exhibit 149 is
7 received as pages one through ten. All right.
8 And did you have any further testimony?

9 MR. ROTE: That's it. That's it.

10 ARBITRATOR CROW: Okay. And you had --

11 MS. MARSHALL: I have one question.

12 ARBITRATOR CROW: A question or two? All
13 right.

14 Q. BY MS. MARSHALL: I have a question of Mr. Rote.
15 Isn't it true that after you testified in this
16 arbitration in June, that NDT, you, actually
17 disclosed of all of the computers from the NDT
18 call center? You did that in July of this year;
19 right?

20 A. Yes. What was remaining, we had in storage for
21 two years and they were disposed this year.

22 MS. MARSHALL: That's all my questions.

23 ARBITRATOR CROW: Okay. Let's go off the
24 record.

25 (Break taken from * to *.)

♀

151

1 ARBITRATOR CROW: Tim, do you want to come
2 closer to the phone.

3 MR. ROTE: Sure.

4 ARBITRATOR CROW: Do we have a notary, Anna?
5 Is there anyone with you?

6 THE WITNESS: Yes. I have a notary here.
7 Do we want to handle this on the speaker or do
8 you want me to hand the phone to him?
9 ARBITRATOR CROW: If the notary will swear
10 you, that will take care of the problem.
11 SPEAKER: Hello, this is Tim.
12 ARBITRATOR CROW: Tim, are you the notary?
13 SPEAKER: Yes, sir, I am.
14 ARBITRATOR CROW: Will you swear Ms. Kloehn
15 to tell the truth and nothing but the truth in
16 this proceeding, please?
17 ** ** sworn sworn ** **
18 ARBITRATOR CROW: Thank you. Go ahead,
19 Mr. Rote.
20 SPEAKER: That's all you need?
21 ARBITRATOR CROW: That's all we need from
22 you.
23 SPEAKER: Have a great day. Go Ducks.
24 THE WITNESS: Hello?
25 Q. BY MR. ROTE: Hi, Anna. Why don't you start out

♀

152

1 by telling us how long you've been with the
2 company and what position you hold right now.
3 A. I have been with the company since October of
4 2001 and I am currently the quality assurance
5 manager.
6 Q. Okay. And you held that position for quite some
7 time. When did you, when did you first get that
8 position?

11-5-10

- 9 A. I have been in the quality assurance position
10 since the end of 2002.
- 11 Q. And you've been the quality assurance manager
12 for that time?
- 13 A. No. I've been the head of the quality assurance
14 department, however I'll only been the manager
15 for about two and a half years, with that
16 official title.
- 17 Q. You were heading up the department prior to that
18 time?
- 19 A. Correct.
- 20 Q. Okay. And kind of describe for us, if you will,
21 your job as a quality assurance manager. What
22 do you do?
- 23 A. Sure. The quality assurance manager basically I
24 oversee the other members of the quality
25 assurance department. And what we do is we look

♀

153

- 1 to the sales, the nonsales, basically the daily,
2 the interactions between the representative that
3 works for NorthWest and the customers and
4 listening to recorded and live calls.
- 5 Q. And in the case in the case of live calls you
6 also determine whether or not those calls
7 satisfy our clients' requirements; is that
8 correct?
- 9 A. Correct, listening to the calls to make sure
10 that they meet all requirements to be valid
11 sales and just all around good calls.

- 12 Q. All right. You were working in Eugene this
13 entire time, from October 2001 forward?
- 14 A. I worked in Eugene, yes, the entire time.
- 15 Q. Okay. In October of 2003 you were working also
16 in Eugene?
- 17 A. Yes.
- 18 Q. And I'm just going to kind of get to the direct
19 question now. Mr. Zweizig has maintained in his
20 testimony that he contacted you I think in
21 approximately October 24th, 2003, to ask you
22 about a schedule referred to as an adjusted
23 hours schedule and to confirm with you that the
24 information reported on that schedule was
25 reported to our clients. Did Mr. Zweizig ever

♀

154

- 1 contact you with respect to this matter?
- 2 A. No. No.
- 3 Q. Do you have access, did you have access at that
4 time to client reports or any information with
5 respect to client reporting?
- 6 A. Not to client reporting, no.
- 7 Q. At what point in time, at some point in time did
8 you acquire access to client reports?
- 9 A. I did. It was a couple years later.
- 10 Q. Okay.
- 11 A. Probably early 2005.
- 12 Q. And how do you remember the context of that?
13 How do you remember that?
- 14 A. I remember that because it was after the absence

15 of the facility manager, at that point when he
16 was no longer able to do reports, I had taken
17 over part of the reports.

18 Q. Okay. No more questions?

19 ARBITRATOR CROW: Cross-examination, Anna.
20 Hold on.

21 Q. BY MS. MARSHALL: Yes. Ms. Kloehn, just to
22 correct the record, I believe Mr. Zweizig
23 testified that he contacted someone he thought
24 it was you. Who in the Eugene call center in
25 October of 2003 would have been the person that

♀

155

1 had access to reports and records relating to
2 hours called?

3 A. In 2003 the facility manager would have been the
4 one in charge of reports.

5 Q. Okay. And who would that be?

6 A. That was Bret *Mullins.

7 Q. Okay. Now, am I correct, did I hear you
8 correctly that you are now responsible for
9 reviewing the veracity of reports?

10 A. For one of the reports, yes.

11 Q. Okay. What report are you responsible for now?

12 A. That would be the Allstate motor club report.

13 Q. All right. And what do you review it for?

14 A. To basically make sure that the information is
15 accurate, matches what we actually did for the
16 day, number of hours, number of sales and
17 support goes to the client.

11-5-10

- 18 Q. Okay. How long has it been since Allstate -- Is
19 that a requirement, by the way, of Allstate
20 motor company?
- 21 A. Honestly, I believe so. I don't know anything
22 about the contract with Allstate motor club.
- 23 Q. All right. Do other, do you know whether other
24 clients require that a person like you, a
25 quality assurance person, review the reports to

♀

156

- 1 make sure that they are being billed for actual
2 hours?
- 3 A. We do have other people that do that. But
4 again, I don't know what's in the contract, if
5 it's required or just that the client likes it.
- 6 Q. Okay. It's all driven by the contract, is that
7 it?
- 8 A. Yes.
- 9 Q. Okay. Well, let me ask you, back in 2003, what
10 was your position then?
- 11 A. It was quality assurance supervisor.
- 12 Q. Okay. When you were the quality assurance
13 supervisor, if information came to your
14 attention that led you to believe that the
15 company may be adding hours to its bills, hours
16 that were not worked, all right, if that had
17 come to your attention, information that led you
18 to believe that that might be happening, would
19 that be something that you would take to your
20 manager?

21 A. If that was happening, then yes, I would have
22 taken it to my manager.

23 MS. MARSHALL: Okay. I have no other
24 questions.

25 ARBITRATOR CROW: Anything further,

♀

157

1 Mr. Rote?

2 MR. ROTE: No redirect. Thank you.

3 ARBITRATOR CROW: Thank you Ms. Kloehn. You
4 can hang up now. We're through with you.

5 MR. ROTE: Go see the kids. Thanks, Anna.

6 THE WITNESS: Thank you. Bye.

7 ARBITRATOR CROW: And you are now finished
8 with your testimony, Mr. Rote, is that so?

9 MR. ROTE: I am.

10 ARBITRATOR CROW: And I understand,
11 Ms. Marshall, that you have a witness.

12 MS. MARSHALL: We have a witness.

13 ARBITRATOR CROW: Come right on down here if
14 you will, sir.

15 MS. MARSHALL: And we want to make sure that
16 your voice picks up on this phone right here.
17 Okay.

18 ARBITRATOR CROW: Mr. Zweizig, are you still
19 there? Max, are you there?

20 MR. ZWEIZIG: Yes, sir.

21 ARBITRATOR CROW: All right. Thank you.

22 ** ** sworn sworn ** **.

23 Q. BY MS. MARSHALL: And your name is?

- 24 A. Chris Cox.
25 Q. Okay. Were you employed by NDT or NorthWest

158

- 1 Direct approximately 2001 to approximately
2 December 9th of 2003?
3 A. Yes.
4 Q. Okay. And you worked with Mr. Zweizig; is that
5 correct?
6 A. Yes.
7 Q. Okay. I'm going to kind of jump around because
8 we're all eager to get out of here.
9 A. All right.
10 Q. I want to ask you about timesheets. Did you
11 ever have a problem with timesheets?
12 A. I always had a problem with timesheets. I
13 didn't do them well.
14 Q. And what was Mr. Zweizig's position with respect
15 to timesheets and you?
16 A. He told me to do my timesheets.
17 Q. Okay.
18 A. And I just kept on failing to do them. I would
19 do them for a while but then, you know, business
20 would creep up and I'd forget to.
21 Q. We're lawyers. We know how that is. Okay. At
22 some point you became aware that Mr. Zweizig had
23 been terminated; is that correct?
24 A. Yes.
25 Q. Okay. Now, it's been a while. So I'll just

159

- 1 tell you that his last day with the company was
2 November 14, 2003.
- 3 A. Okay.
- 4 Q. Did you become aware that he was going to be
5 terminated before that date?
- 6 A. I think yes, I was called to a meeting and I was
7 told that he was going to be fired or let go.
- 8 Q. Okay. And do you remember exactly when that
9 meeting was or can you just --
- 10 A. I couldn't tell you exactly when that meeting
11 was.
- 12 Q. Can you say a couple of weeks or whatever?
- 13 A. My guess would probably be a couple of weeks
14 prior to him being let go, but yeah.
- 15 Q. Okay. In this meeting, where was the meeting,
16 by the way?
- 17 A. At Tim Rote's house.
- 18 Q. Okay. And was there anybody there other than
19 Mr. Rote?
- 20 A. No.
- 21 Q. Did he tell you that you would be replacing
22 Mr. Zweizig?
- 23 A. Yes.
- 24 Q. And how did you feel about that?
- 25 A. I mean, it felt good that I would be, I mean, I

♀

1 would be going up in the position. But at the

11-5-10

- 2 same time it was a logical choice, I think, for
3 me to take over the position. So I wasn't
4 surprised.
- 5 Q. Sure. Okay. At that point who all was in the
6 IT department?
- 7 A. Our IT department was pretty small. It was just
8 Max and I.
- 9 Q. Okay.
- 10 A. And, no wait a minute. There was another
11 fellow, I think he came on recently. I don't
12 remember his name. So there was three of us at
13 a time. But 95 percent of the time I worked
14 there it was just Max and I.
- 15 Q. All right.
- 16 A. I would say.
- 17 Q. At some point between the time that you learned
18 that you would be taking over Mr. Zwei zig's
19 tasks and when he left, you actually gave notice
20 that you would be leaving the company?
- 21 A. Yeah.
- 22 Q. Is that correct?
- 23 A. That is true.
- 24 Q. Was that a voluntary resignation?
- 25 A. Yes, it was. I was just looking to go into

♀

161

- 1 something different. Dot net programming was
2 just coming out and that was a new thing and I
3 felt that would be a great career path me and I
4 had an opportunity to take it, so I did.

11-5-10

- 5 Q. Okay. Did Mr. Zweizig have anything to do with
6 your decision to leave?
- 7 A. No.
- 8 Q. Do you know a fellow by the name of Joe Ci offi ?
- 9 A. He e-mailed me a couple times after I left
10 NorthWest Di rect.
- 11 Q. Was he employed there while you were there?
- 12 A. I don't believe so, no. No.
- 13 Q. So if Mr. Zweizig, if his last day was
14 November 14th and your last day was
15 December 9th, you were the guy for approximately
16 three weeks; is that correct?
- 17 A. Yeah.
- 18 Q. Remember that?
- 19 A. I, that would be safe to assume, yes. Yeah. I
20 mean, you would think -- Yeah, I was. I was the
21 man between, for that three weeks.
- 22 Q. So you should be able to tell us whether the
23 company ever shut down after Max left while you
24 were there because of anything that he did or
25 di dn' t do.

‡

162

- 1 A. No. The company never shut down.
- 2 Q. Do you remember anyone ever coming to you and
3 asking you to find any programs that Mr. Zweizig
4 had written or used?
- 5 A. No, I don't remember.
- 6 Q. Okay.
- 7 A. Bei ng, speci fi cal l y bei ng asked to do that. But

11-5-10

8 then again, I mean, looking for programs on a
9 server every day and stuff like that would have
10 been something that I did.

11 Q. Okay. Well, during the period where you were
12 the only IT guy?

13 A. Yes.

14 Q. Or you and perhaps one other person, do you
15 remember there being any angst or sense of
16 urgency to search for Mr. Zweizig's programs?

17 A. No, I don't.

18 Q. Okay. If you had been asked to look for
19 Mr. Zweizig's programs, the ones that he wrote,
20 where would you look?

21 A. The programs would exist on the EIS server.

22 Q. Okay.

23 A. And there would be a Windows 98 computer that
24 had a directory with all of Max's programs in
25 it.

♀

163

1 Q. Okay. Did you personally ever have occasion to
2 access those programs?

3 A. Did I?

4 Q. Yeah.

5 A. Yeah.

6 Q. Can you tell us a little bit about the programs.
7 Were these Fox Pro programs?

8 A. They were Fox Pro programs, simple programs that
9 just did, the EIS programs usually did reports.
10 He had a couple programs that would extract data

11 for processing and you'd probably have a few
12 Windows appears that would pull data from the IS
13 server over, either create a report right there
14 for them or produce processing data for our
15 clients.

16 Q. Okay. Now, how would you, how would you
17 characterize these reports? Were these kind of
18 stock reports that would apply over a broad
19 variety of situations or how would you
20 characterize them?

21 A. Usually each program was designed for each
22 campaign. And the campaign would evolve based
23 on Bret's needs or the client's needs. So they
24 would always be changing based on a different
25 campaign. And you would adjust them accordingly

♀

164

1 to what they wanted. Same thing with
2 processing, probably less, to a lesser extent
3 than the reports.

4 Q. Okay. Now, you, you were primarily responsible
5 for scripting, for programming and scripting; is
6 that correct?

7 A. Scripting was mainly mine, yeah.

8 Q. Okay. Did, prior to you leaving did you have
9 occasion to train anybody in preparing scripts?

10 A. I think I started training Rory, but he wouldn't
11 have been qualified to do much by the time I
12 left.

13 Q. Okay. And so you were handling both yours and

- 14 Max's job and you were training Rory. Were you
15 training anybody else?
- 16 A. No. Well, there was another, there was that
17 other IT guy, I forget what his name was, and he
18 was doing work as well. And I believe he was
19 learning scripting as well, too. But, I mean,
20 daily business, I didn't do a lot of training,
21 no.
- 22 Q. Yeah. What can you tell us about the IT
23 department once you were gone?
- 24 A. Once I was gone, the IT staff was pretty slim.
25 They wouldn't need to be replaced right away. I

♀

165

- 1 mean, there was only three of us at the time.
- 2 Q. Okay.
- 3 A. Came down to one.
- 4 Q. I'd like to have you look at Exhibit 128, pages
5 one and two. Can you tell me where that is. It
6 might be over here. Just make sure it is.
- 7 MR. MARSHALL: You keep taking them away
8 from me.
- 9 MS. MARSHALL: Sorry. It's my fault.
- 10 Q. BY MS. MARSHALL: Well, I'll let him look for
11 that and I'll ask you another question.
- 12 Mr. Crow, do you have Exhibit 128?
- 13 ARBITRATOR CROW: Yeah, I do.
- 14 MS. MARSHALL: Would you mind sharing it
15 with the witness because I only have about three
16 questions left.

- 17 MR. MARSHALL: Here it is.
- 18 Q. BY MS. MARSHALL: All right. Exhibit 128,
19 there's been some testimony about this and
20 basically some questions about what page 1 and
21 two are. Can you just explain it for us what
22 page 1 and two is.
- 23 A. All right. So the password to Max... We pass
24 passwords around via e-mail quite often because
25 they weren't written down and, in a specific

166

- 1 location. It's probably best that they weren't.
2 So if you forgot a password or a new machine
3 came on line or we changed a password or you
4 haven't been on a certain machine in a long
5 time, I would e-mail Max and ask him for
6 passwords. He would probably e-mail me and ask
7 me for passwords.
- 8 Q. Okay.
- 9 A. And that's all that is basically.
- 10 Q. Were you the keeper of the passwords?
- 11 A. We didn't have a keeper of the passwords. But,
12 so no. I mean, there's two schools of thoughts
13 on keeping passwords. One is if you keep your
14 password in a file then somebody steals it and
15 you get all your passwords. The other thing is
16 if you don't keep any passwords, they're secure
17 that way. And that's the way we went because
18 it's the way most companies do go, I think.
- 19 Q. Did either of you have access to the

11-5-10

- 20 administrative server as a practical matter?
- 21 A. Yeah. We had access to all servers.
- 22 Q. Okay. Why don't you tell us what the second
- 23 page is.
- 24 A. This would be just a spoof that was sent to Max.
- 25 The subject says, Chris in, I think he wanted me

‡

167

- 1 to send him an e-mail every morning when I was
- 2 getting in and of course being smart about it I
- 3 wrote a program that sent him an e-mail at 8:00
- 4 in the morning.
- 5 Q. So it was sort of a joke?
- 6 A. Yeah. It was kind of a joke, you know. And,
- 7 that's all that is.
- 8 Q. Okay. Well, the reason it's come up is that
- 9 there's some question about whether Mr. Zweizig
- 10 improperly accessed data in the administrative
- 11 server before he left. Did you have any
- 12 awareness of that?
- 13 A. No.
- 14 Q. Okay. And speaking of passwords, did you do
- 15 anything to prevent Mr. Zweizig from accessing
- 16 information after he left?
- 17 A. Yes. We had a lock-out procedure that Max and I
- 18 discussed. If any of us was terminated, that we
- 19 would make sure that was done right away.
- 20 Q. Okay. And what's that mean, a lock-out
- 21 procedure?
- 22 A. It means you'd go in, you'd go into every single

23 computer, every PC Anywhere, any access like
24 that and you would change the password to
25 something they didn't know so they couldn't log

‡

168

1 in, basically lock them out.
2 Q. Okay. Going back to you going to the
3 administrative server to get Mr. Zweizig's Fox
4 Pro programs.
5 A. Okay.
6 Q. If the administrative server happened to be down
7 or crashed or something like that, was there any
8 back up?
9 A. The EIS server is backed up every night on the
10 tape. And the Windows 98 box that held the
11 programs had a batch file that would run on a
12 scheduled job within the machine. It would
13 actually take a folder, it would copy it to the
14 other drive. So the chances of both drives
15 going bad at the same time would be very slim.
16 So you could get the programs back out off the
17 other drive. So yeah, they were backed up.
18 Q. So if you knew what you were looking for, that
19 would be where you'd go to look for them?
20 A. Uh-huh.
21 Q. Is that right? Okay. Well, let's say you still
22 couldn't find them. You couldn't find
23 Mr. Zweizig's Fox Pro programming on the server
24 and you couldn't find them in the backup tapes.
25 What would you do then?

1 A. If you couldn't find the program at all, you
2 would have to write it from scratch.

3 Q. Would that be a problem?

4 A. No I don't -- No. None of the programs were so
5 extensive that they would take a long time to
6 recreate. Some of the processing programs were
7 more involved, but no, I don't believe so.

8 MS. MARSHALL: Okay. I have no other
9 questions.

10 ARBITRATOR CROW: Mr. Rote.

11 Q. BY MR. ROTE: Back when you tendered your
12 resignation, you noted that you did so for
13 health reasons, that you were stressed and for
14 health reasons. Do you remember that being a
15 stressful time?

16 A. Oh, yeah.

17 Q. Very stressful?

18 A. It was very stressful.

19 Q. Do you remember a gentleman by the name of Jamie
20 Getty from *Teleformix flying out from Chicago
21 and working with us for a period of time?

22 A. Jamie Getty.

23 Q. From Chicago, a company called *Teleformix?

24 A. Jamie Getty. *Teleformix. No, I don't.

25 Q. You don't.

- 1 A. No, I don't.
- 2 Q. Okay. Do you remember the other party employee,
3 *Gunowen *Darmatti?
- 4 A. Is that the one I'm thinking about? Yeah. That
5 one.
- 6 Q. I think so. I think that's the one you are
7 thinking of?
- 8 A. That's the other employee that I am missing,
9 *Gunowen.
- 10 Q. Now you had experience with Visual Basic and
11 database programs like Fox Pro or SQL?
- 12 A. Server.
- 13 Q. SQL. And was it your understanding that
14 *Gunowen also had experience with those same
15 kind of things?
- 16 A. Yeah.
- 17 Q. And so essentially there were three people in
18 the department at that time, you, *Gunowen and
19 Max?
- 20 A. Correct.
- 21 Q. And if the company had substantially expanded,
22 let's say increased by 50 percent, would you say
23 that we'd have to add substantially more staff?
- 24 A. We would. In the IT department? Yeah.
- 25 Q. In the IT department.

♀

- 1 A. I would, I would think you'd have to add on,
2 yeah, I think you would.

11-5-10

- 3 Q. So the fact that we have three people today and
4 we're substantially bigger, would you say that
5 that means that we are much better at database
6 processing, scripting? What would you think
7 that would mean?
- 8 A. You know, it's tough to say, if you were going
9 to hire -- At the time I guess I was a junior
10 level programmer. I mean, if you were to hire
11 me today I could probably do the work of two or
12 three more people. I think my experience has
13 just grown that much. But back then it felt
14 like, yeah, you would have had to hire more
15 people.
- 16 Q. The, kind of go back to kind of the stressful
17 time when you decided to resign. Can you kind
18 of describe for us what was causing the stress?
- 19 A. There was just a lot of stress between Max, you,
20 Brent *Cowiak, it seems like there was always a
21 conspiracy going on. And it was just normal
22 business. And it was hard to deal with that
23 because everybody was working so hard and all it
24 was was just normal business and there was
25 nobody trying to do anything extraordinary or, I

♀

172

- 1 mean, out of the ordinary, I would say.
- 2 Q. Would you say that friction was going on for a
3 while?
- 4 A. Oh, yeah.
- 5 Q. It had gone on for quite a while?

11-5-10

- 6 A. Uh-huh.
- 7 Q. So at the time that you resigned, however, that
8 was after Max's last day.
- 9 A. Yeah.
- 10 Q. It was quite a bit -- And that stress continued
11 to go on if not get greater after his last day.
- 12 A. (No audible response.)
- 13 Q. Now, remembering that then state of mind at that
14 time, does it jog your recollection about Jamie
15 Getty from Chicago coming in to help us with a
16 number of matters?
- 17 A. I'm sorry. I don't remember Jamie Getty.
- 18 Q. All right. That's fine. You were asked about a
19 meeting that you attended with me when we
20 discussed Max's departure or termination. And,
21 but you don't recall the exact date when that
22 happened, do you?
- 23 A. Oh, no.
- 24 Q. No. But it wasn't, would you say it was not the
25 first time that we talked about issues and you

♀

173

- 1 assuming command of the department?
- 2 A. No. It probably wouldn't have been the first
3 time, no.
- 4 Q. We had had other conversations about you
5 assuming the reins of the department. Do you
6 remember the concerns being that we just wanted
7 someone here, on the ground here taking control
8 of the department, manage being the department?

9 A. Yeah.
10 Q. As opposed to in New Jersey?
11 A. I remember you saying that. Yeah.
12 MR. ROTE: No more questions.
13 ARBITRATOR CROW: Redirect.
14 MS. MARSHALL: No. No questions.
15 ARBITRATOR CROW: Thank you, Mr. Cox. You
16 are free to leave.
17 THE WITNESS: All right. Thank you.
18 MR. ROTE: Thank you, Chris.
19 THE WITNESS: Nice meeting you.
20 MS. MARSHALL: Thank you.
21 ARBITRATOR CROW: And I gather that we have
22 come to the end; is that correct.
23 MS. MARSHALL: As I said, all good things
24 have to come to an end.
25 ARBITRATOR CROW: It's a shame, but I guess

♀

174

1 it happens. Okay. Then we can go off the
2 record.
3
4
5
6
7
8
9
10
11

11-5-10

12
13
14
15
16
17
18
19
20
21
22
23
24
25