13   The Defense may call its first witness.

14   MR. KURTZ: Thank you, Your Honor. At this time the

15   Defense calls Special Agent Gregory Johnson.

16   WHEREUPON,

17   GREGORY JOHNSON,

18   being first duly sworn, was examined

19   and testified as follows:

20   DIRECT EXAMINATION

21   BY MR. KURTZ:

22   Q.   Good afternoon, Special Agent Johnson.

23   A.   Good afternoon.

24   MR. KURTZ: May I approach the witness, Your Honor?

25   THE COURT: You may.

1   MR. KURTZ: Actually, I -- I would ask, given the

2   State has previously qualified Special Agent Johnson as a

3   computer forensics expert, if we -- we tender him as such at

4   this time.

5   THE COURT: He's already been offered and testified

6   as such in this matter. You may proceed.

7   MR. KURTZ: Thank you. Approach the witness?

8   THE COURT: You may.

9   BY MR. KURTZ:

10   Q.   Special Agent Johnson, I'm showing you what's been

11   marked as Defendant's Exhibit 118. You have evaluated the

12   MFT, which is the master file table, of the IBM ThinkPad,

13   correct?

14   A.   That's correct.

15   Q.   And in doing so, you evaluated the files that were

16   created during the July 11th dated search on Google Maps?

17   A.   That's correct.

18   Q.   Among the files were the open hand and --

19   MR. ZELLINGER: Objection to leading, Your Honor.

20   MR. KURTZ: I'd ask to be able to treat Special

21   Agent Johnson as a hostile witness. He is the FBI.

22   THE COURT: He -- he hasn't demonstrated the need

23   for that at this point. The objection's sustained.

24   BY MR. KURTZ:

25   Q.   Do you recognize those as being files from the

1   master file table on the IBM ThinkPad?

2   A.   Yes.

3   Q.   And have you evaluated files from Google Maps in

4   the past under any other circumstances?

5   A.   Yes.

6   Q.   Are you familiar with the -- the open hand and

7   closed hand artifact from Google Maps?

8   MR. ZELLINGER: Objection to the leading, Your

9   Honor.

10   THE COURT: Overruled. He did not suggest the

11   answer in that question, so it's not a leading question.

12   A.   Could you please repeat that?

13   BY MR. KURTZ:

14   Q.   Are you familiar with the open and closed hand

15   cursors from Google Maps?

16   A.   Yes.

17   Q.   At the end of a file name, there is a period and

18   then three letters, correct?

19   A.   That's correct.

20   Q.   What does the -- what do the three letters at the

21   end designate?

22   A.   The type of file that the file is. It's called a

23   file extension.

24   Q.   And on the IBM ThinkPad, what are the extensions

25   for the opened and closed hand cursors that appear in the

1 MFT?

2   A.   I'm assuming their BMP.

3   Q.   In your experience, have you encountered a .CUR

4 extension for cursors?

5   A.   I'm sure I have, but I don't -- I don't recall

6 anything specific about those.

7   MR. ZELLINGER: Your Honor, at this point I'd ask,

8 if Mr. Kurtz isn't using the exhibit, that he return to his

9 table.

10   MR. KURTZ: I am actually using the exhibit.

11   THE COURT: Go ahead.

12   BY MR. KURTZ:

13   Q.   Now, Special Agent Johnson, when someone uses the

14 cursors in Google Maps, can you explain their function, how

15 somebody is using those?

16   A.   Well, do you mean on the -- on the map itself, as

17 it was in this situation?

18   Q.   How -- in general, how is it that somebody uses

19 that opened and the closed hand?

20   A.   Okay. I -- I believe Officer Chappell explained

21 it, but basically, when you hover over the map portion of the

22 -- of the Google Maps -- [cleared throat] excuse me -- your -

23 - your -- your pointer or your cursor, which actually,

24 typically on most computers, is a -- is a pointer, will

25 change into the -- into the open hand designation and it

1 | looks like a little -- little white glove pointing.

2 | And then when you go to move the map to the area

3 | that you want to expand on or move into, it -- it will

4 | actually go into a closed hand, indicating that you are

5 | grabbing, you know, much like you would this piece of paper,

6 | like I'm grabbing it and -- and pulling it over. Is that --

7 | is that what you mean?

8 | Q.   Yes, sir.

9 | A.   Okay.

10 | Q.   And when you do that, when is that file created on

11 | your system?

12 | A.   On -- on the tests that -- that we ran, it was not

13 | created until we grab -- grabbed the page to manipulate the

14 | page over.

15 | Q.   And so you actually ran a test where you -- you

16 | grabbed one section and pulled it over?

17 | A.   That's correct.

18 | Q.   How is -- how is Google using that cursor? Do you

19 | know how it functions within Google? Is it something that it

20 | creates new ones for every pixel?

21 | A.   No. It was -- it was our understanding in -- in

22 | the way that we were able to replicate it that, no, it -- it

23 | would just -- it created at -- at the time it was -- it was

24 | first created or first used.

25 | Q.   And then, is that cursor in use up until the point

1 where the screen stops moving, until you let go?

2   A.   Used as, what do you mean? Used, as in how?

3   Q.   Is -- does Google interact with that cursor -- does

4 your computer interact with that file that it's placed on

5 your computer from the moment you start until the moment you

6 finish using it?

7   A.   I'm -- I'm not really -- I'm not really sure what

8 you're asking, I guess.

9   Q.   Well, if you look --

10   A.   Do you mean, is it still on the screen? Is -- is

11 your cursor still in the form of --

12   Q.   Is it --

13   A.   -- one of -- one of these two cursors?

14   Q.   -- is it still on the screen, is the first

15 question.

16   A.   Yes.

17   Q.   Is that file actually still being used by the

18 computer? Is -- is it still in use?

19   MR. ZELLINGER: Objection. Leading, Your Honor.

20   THE COURT: Overruled.

21   A.   Yes, it's -- it's still -- it's still being used,

22 as far as if it's still being -- if it's still on the screen.

23   Q.   In your memory, basically.

24   A.   Yes. Yes.

25   Q.   If you would, could you indicate what the standard

1   information create date is for the -- for the open hand file,

2   which I believe would be the first category.

3   A.   The standard information create date?

4   MR. ZELLINGER: Your Honor --

5   Q.   Yes.

6   MR. ZELLINGER: -- I'd object. Is that question

7   based on the document that it was given, or based on his

8   examination?

9   MR. KURTZ: I believe it's based --

10   THE COURT: I believe --

11   MR. KURTZ: -- on --

12   THE COURT: -- he's asking off -- by Defendant's

13   118, it I'm not mistaken.

14   MR. KURTZ: That is correct, Your Honor.

15   MR. ZELLINGER: Well, Your Honor, I don't believe

16   there's been a proper foundation for Defendant's Exhibit 118

17   at this point.

18   THE COURT: Can you ask some foundational questions

19   with respect to 118?

20   BY MR. KURTZ:

21   Q.   Do you recognize these as in fact being part of the

22   master file table from the IBM ThinkPad computer?

23   A.   I mean, they appear to be, without comparing them

24   to, you know, to our listing. I mean, I'm assuming that you

25   -- you pulled them off accurately. All the information is --

```
 1   is accurate.
 2        Q.    Would it --
 3        A.    But I --
 4        Q.     -- help --
 5        A.     -- I don't know.  I -- I didn't make this
 6   document, so I don't -- I don't know, but I'm assuming that
 7   that is correct.
 8        Q.    Would it help you to take a look at --
 9        A.    Sure.
10        Q.     -- the actual -- okay.  So, Special Agent Johnson,
11   could you tell me what time that document reflects as the
12   standard information create date?
13        A.    For the -- the first file name?
14              MR. ZELLINGER: Your Honor, I'd object to doing this
15   in front of the jury.  I gave Mr. Kurtz my copy, but there's
16   been no foundation for that time at this point.
17              THE COURT: Can you refer to the document, either up
18   --
19              MR. KURTZ: Fine.
20              THE COURT:  -- here or there?
21              MR. KURTZ: Yes, Your Honor.
22        BY MR. KURTZ:
23        Q.    Special Agent Johnson, do you know if yours is in
24   UTC or in Eastern Standard?
25        A.    These appear to be in UTC.
```

1   Q.   Okay.

2   MR. ZELLINGER: Your Honor, can I look at them?

3   THE COURT: You may.

4   (Mr. Zellinger examines the exhibit.)

5   BY MR. KURTZ:

6   Q.   Special Agent Johnson, you are welcomed to -- to

7 navigate any way you like. Is this in fact the MFT that

8 y'all provided through discovery?

9   A.   Yes.

10   Q.   Now, looking -- I believe I highlighted -- is it

11 the closed hand?

12   A.   Yes.

13   Q.   Now, if you would please look at the standard

14 information create date, and actually matching them up

15 against all values, are all of the values that are on that

16 sheet accurate but for the fact that they don't go to the

17 millionth of the second, that they go to the thousandth of a

18 second?

19   A.   Yes.

20   MR. KURTZ: At this point, Your Honor, I would ask

21 to admit Defendant's Exhibit 118 as being an accurate

22 representation of the open and closed hand files, including

23 standard information, access time, modification time, access

24 time, and entry modified time, as well as file name

25 categories.

```
 1              THE COURT: Any objections?

 2              MR. ZELLINGER: Well, Your Honor, I just object

 3    because the -- what's on the Defendant's Exhibit 118 is not

 4    identical to what the tests the FBI performed, but it's down

 5    to the millionth of a second, so it's not --

 6              THE COURT: Overruled.  I'm going to admit it.

 7         BY MR. KURTZ:

 8         Q.   So, Special Agent Johnson, if you would take a look

 9    at where it says standard information create date, what time

10    is that for the open hand?

11         A.   It's 17:14:53.

12         Q.   And the thousandths of a second are .891?

13         A.   Yes, sir.

14         Q.   And what is the time for the modification?

15         A.   The standard modification, start   --

16         Q.   Standard information modification.

17         A.   It's -- it's the same time, 17:14:53.

18         Q.   And when is that time noted for the standard

19    information access?

20         A.   Same time, 17:14:53 point eight -- 891.

21         Q.   Are all of those numbers also the same for all four

22    of the file stamp times in the file name information

23    category?

24         A.   Yes, they are.

25         Q.   And then, looking down at the closed hand, what --
```

```
 1   well, the easier question is, are all of the times identical
 2   for the closed hand as well?
 3        A.   Yeah, it's -- it's a different time than the open
 4   hand, but yes, they are all identical, with the exception of
 5   the info entry day.
 6        Q.   Now, what we had discussed was that when you first
 7   create a file, it would -- at that point, is that when this
 8   date is created?
 9        A.   On the computer, yes.
10        Q.   And then, as you use the file, the file is still
11   being accessed, correct?
12             MR. ZELLINGER: Your Honor, I object to the leading.
13             THE COURT: That was a leading question.  If you can
14   rephrase the question.  You said "correct."  It's a -- it's a
15   question that suggests the answer.
16             MR. ZELLINGER: I hear you, Judge.  I'm just trying
17   to think of how to ask the question.
18        BY MR. KURTZ:
19        Q.   If you navigate from one place to another, what
20   happens with the files that you're working with on the
21   computer?
22        A.   Well, it -- it depends on -- on the file.  In this
23   case, the file is not really being modified.  This -- these
24   are the dates that the file is being sent down from Google to
25   the -- to the local machine.
```

1   Q.   Uh-huh.

2   A.   So I wouldn't expect until -- until you maybe

3   navigated away from the page and came back and maybe you

4   would see this open hand one incremented by one, which would

5   be maybe then a two. I wouldn't expect these dates to -- to

6   change.

7   Q.   Have you tested that?

8   A.   I don't -- I don't think we tested that in relation

9   to the times, no. When we tested it, we were trying to

10   figure out when exactly you would get the -- the file, these

11   open hand and the closed hand, sent down to your computer,

12   what action would dictate that happening. But as far as the

13   times, no.

14   Q.   Is it possible that moving a cursor from one place

15   to another could result in the computer showing time as being

16   accessed?

17   MR. ZELLINGER: Objection to the leading. It

18   suggests the answer in the question.

19   THE COURT: Overruled.

20   A.   Again, it would -- it would depend on the file

21   itself. A -- a BMP file, I'm -- I wouldn't necessarily

22   expect that to happen. A -- a BMP file is a -- is an image-

23   type file. It's not like a -- a JavaScript file or something

24   that would have code associated with it, if that makes sense.

25   Q.   Is this a particularly difficult thing to test?

A.   I wouldn't think so, no.

        Q.   Is there any reason why we can't do that right
here, right now, with this machine?

        A.   I would -- I'd prefer if it was a clean machine
that maybe had never been on the internet before. You would
need internet access and -- and download it from Google and -
- and, beyond that, I'm not so sure that Google would even
still use the same technology as they did before. So if the
results were -- if the results were different, I would -- it
would kind of give me pause.

        Q.   The tests that -- that you did recently -- you did
testing on the machine as early as last week, didn't you?

        A.   Not -- not in conjunction with the Google stuff.

        Q.   Okay.

        A.   Not -- not with the Google files.

        Q.   Would you expect BMPs or CURs to react differently
today than they would have acted? Do you have specific
reason to believe that that is the case?

        A.   That they would have acted when? That --

        Q.   In July of 2008.

        A.   I -- I wouldn't expect them to, however, you know,
it would be impossible for me to tell.

        Q.   Well, I -- I would ask if you would please attempt
to replicate the -- by clearing out internet history --

        A.   Uh-huh.

1   Q.   -- and navigating Google maps to see if this

2   machine responds similarly.

3   MR. ZELLINGER: Your Honor, I'm going to object to a

4   forensic examination of Mr. Kurtz computer being conducted

5   right now in courtroom 3-C.

6   THE COURT: Sustained.

7   MR. ZELLINGER: It's -- it's not a forensic exam,

8   Judge. It's a test that takes minutes.

9   THE COURT: How can we be assured that it -- it's

10   the exact same conditions -- if the -- are you using a

11   different type of computer? Does it have different software

12   and programs? I don't understand how you can replicate it

13   without that and that's why I'm sustaining the objection.

14   MR. KURTZ: Well, I'd like to be heard, Your Honor.

15   THE COURT: Members of the jury, I'm going to ask

16   you to step to the jury room for a minute. I'll have you

17   return to the courtroom when we are through with this matter

18   outside your presence.

19   (The jury left the courtroom.)

20   THE COURT: Let the record reflect that all members

21   of the jury have left the courtroom. Do you wish to be heard

22   outside the presence of the jury?

23   MR. KURTZ: Your Honor, I'm -- I actually do have a

24   -- a Vista machine that I'm happy to substitute for this

25   computer, which would be a closer match. There is -- I don't

1 believe, any particular reason to believe that the

2 functionality is different in any way and certainly it is

3 relevant. Special Agent Johnson is capable and knowledgeable

4 and would be able to make an observation in a matter of

5 minutes. It certainly wouldn't delay the proceeding in any

6 way and I believe that it would certainly shed light on this

7 question.

8   THE COURT: Yes, sir.

9   MR. ZELLINGER: Your Honor, one, the -- this

10 examination is in no way a -- a forensic examination with

11 proper safeguards. Agent Johnson said that it gives him

12 pause to do this, so I think if the Defendant wants to do

13 this, he needs to call an expert who it doesn't give pause to

14 to conduct an examination on a non-virgin computer in -- in

15 this environment. But Agent Johnson said it gives him pause.

16   Additionally, I wasn't the one who just said that

17 this is not a delaying tactic; that was Mr. Kurtz. Their --

18 I would say under Rule 403 and many other rules of evidence,

19 this is improper because, one, Agent Johnson says that this

20 isn't the environment that he wants to do it in, and; two,

21 it's more prejudicial than probative and that there's --

22 there's no probative value into doing this on Mr. Kurtz's

23 computer.

24   We have no idea what the operating -- what the

25 situation of the operating system is. We don't know if the

```
 1   operating system's the same now as it was in 2008.  There's

 2   all these safeguards that need to be conducted and that's why

 3   we have experts to do it.  And to ask Agent Johnson to do it

 4   from the witness stand, outside of where he feels comfortable

 5   doing it, I think is inappropriate.

 6            MR. KURTZ: Your Honor, I -- I have a Vista machine.

 7   I think I can ask several questions of Special Agent Johnson

 8   on voir dire that would clarify as to the -- the difficulty

 9   of the process.

10            THE COURT: As to this machine, pursuant to Rule 611

11   and Rule 403, I'm going to sustain the objection.  If you

12   want to ask him some questions about a Vista machine at this

13   point, you may.

14            MR. KURTZ: Thank you, Your Honor.

15      BY MR. KURTZ:

16      Q.   Special Agent Johnson, certainly the Defendant's

17   computer was a Vista computer; was it not?

18      A.   That's correct.

19      Q.   And Vista is a unique operating system as compare

20   to a variety of others, like Windows 7 or Windows XP?

21      A.   Yes.

22      Q.   It would be a more relevant comparison to use a

23   Vista machine than that Windows 7 machine?

24      A.   You're getting closer, yes.

25      Q.   Okay.  You don't have any personal knowledge of
```

```
 1   Google changing the way that they interact with the cursor

 2   file over the last two years?

 3        A.   Not the cursor file specifically, no.

 4        Q.   This -- is it a -- is fair to say that all that

 5   would be required to actually perform this test would be to

 6   empty out temporary internet files so that there's nothing

 7   there.  Would that be the first step?

 8        A.   Well, what -- what are we trying to -- what exactly

 9   are we trying to show?  Are you trying to -- if I understand

10   where you're going, I -- I'm assuming that you're trying to

11   show that once the file gets downloaded to the computer, it

12   has a standard information creation date, but when I start

13   moving the file, it's going to change some of these other

14   date -- other times, they would be same.  Is that correct?

15        Q.   That's an accurate statement --

16        A.   Okay.

17        Q.    -- yes, sir.

18        A.   Okay.  So what -- so what's your question?

19        Q.   The question is: To actually conduct an examination

20   to test that, the only steps involved to do it would be

21   clearing out the temporary internet files, going to Google

22   Maps, and navigating the map, and then going back to

23   temporary internet files and checking the timestamps.

24        A.   The only problem with that is, I'm not going to get

25   all -- I'm not going to get all eight timestamp readings
```

```
 1  through your -- right?
 2        Q.    That --
 3        A.    You understand that, right?
 4        Q.     -- that's absolutely right, sir.
 5        A.    Uh-huh.
 6        Q.    Though you recognize that by looking at all eight
 7  timestamp readings, you can see none of them have changed.
 8        A.    On this -- on -- on -- on the printout here?
 9        Q.    Yes, sir.
10        A.    Yes, I can.
11        Q.    So the -- even though -- well, the artifacts on the
12  IBM ThinkPad, they do not reflect any progression in time
13  from the creation date to the modification date, correct?
14        A.    That's correct.
15        Q.    And the question is exactly what -- what you said.
16  The question that I'm asking is: Would you expect to see a --
17  an updated modification time?  And as a result, my question
18  to you is: We would be able to see at least the modification
19  time and the creation time without forensic software, just
20  looking in the temporary internet folder?
21        A.    If -- if those -- if those columns are available,
22  yes.
23        Q.    And you certainly would be able to make those
24  columns available?
25        A.    We could try.  I -- I've never tried to do that
```

1   before, but we'll -- I can try to see if those columns are

2   available.

3   Q.   And this is not something you would expect would be

4   a terribly complicated experiment to conduct?

5   A.   No.

6   MR. KURTZ: Thank you, Your Honor. That -- I think

7   that this is appropriate for the jury.

8   THE COURT: Do you want to be heard?

9   MR. ZELLINGER: I do, Your Honor. We still have the

10   same situation where this isn't in a laboratory where he's

11   attempting to replicate and use a -- a clean computer.

12   Additionally, you've heard from Agent Johnson that

13   when he examines these time columns that are -- you know,

14   usually these computers are shut off and then he's looking at

15   an image copy of the hard drive. I don't think that the

16   protections are there, and I can ask further questions for

17   what the Court needs, but this is simply a delaying tactic.

18   The jury can't even see what this experiments going to be.

19   This is akin to a -- a chemist being asked to replicate on

20   the stand how they determine that something was cocaine. I

21   mean, it's the same thing. It's improper based on Rule 403

22   and that it has very little probative value and it's being

23   used solely as a delay tactic at this point.

24   MR. KURTZ: Judge, I -- I'm happy to extend a -- a

25   cable so that this is entirely something that the jury can

1 see by simply plugging it in the projector, by replicating

2 the screen. The question that Special Agent Johnson

3 understands that I'm asking is, and the bottom line is,

4 whether or not this is proof that somebody placed this file

5 on the machine. That's the question I'm asking.

6   And the -- the bottom line is, if in the history of

7 -- the bottom line is, if the times don't change across the

8 board, and you drag something, there is a start time and

9 there is a finish time. And computers are really good about

10 keeping time when it comes to create and modify. And if the

11 same exact nanosecond appears in every single column, unless

12 for some reason the computer is not updating the file, it

13 indicates placement on the computer at one time as opposed to

14 the natural progression that one would expect when one

15 navigates through the map.

16   And it is a tremendously simple task. It does not

17 require a forensically sound environment. It simply requires

18 clearing out one folder, navigating, and looking back at the

19 folder to see what the time is on it. It couldn't possibly

20 be more relevant and it -- it couldn't possibly be simpler.

21   And what Mr. Zellinger is saying is, well, I could

22 have an expert do it. Well, evidently, no I can't. So I've

23 chosen a gentleman who, if he has any bias, it would be

24 toward the State. The test would be within his command and

25 control. It's not like I'm trying to play smoke and mirrors

1   here. I'm asking a Special Agent with the Federal Bureau of

2   Investigation to conduct a simple, brief experiment. And if

3   it is to get at the truth, I think Mr. Zellinger's claim that

4   this a delaying tactic is absurd.

5   THE COURT: Do you want to be heard?

6   MR. ZELLINGER: I do, Your Honor. First of all,

7   doing this test live can result in inaccurate time results

8   because the access data, when you look at the access data,

9   can change it. This is not a forensically sound environment

10   to do it; Agent Johnson's already said that. There is a

11   million reasons why what might come up on that computer as to

12   the access date and the times and -- and -- and the -- the

13   correlation with the Defendant's expert, why it might not be

14   consistent or why it might not be consistent with what Agent

15   Johnson testifies to. And based on that, Your Honor, there's

16   a huge prejudicial impact of that to jury, and there's no

17   safeguards as to -- we don't know what's on that computer. I

18   mean, we have no --

19   THE COURT: Well, it's not going to be done on that

20   computer. I thought he said he had a Vista computer.

21   MR. KURTZ: I do, Your Honor.

22   MR. ZELLINGER: And, Your Honor, it's just to -- to

23   -- I don't know what computer we're going to use, but we

24   don't know what's on that computer. And -- and to ask Agent

25   Johnson to do this investigation over again on a computer

1 that has a different timing and -- and we don't know what's
2 on it, is -- is inappropriate at this point.
3   I understand Mr. Kurtz's frustration that he -- he
4 offers these time should have been changed according to -- to
5 what he believes. He can ask Agent Johnson that. He can
6 say, shouldn't -- shouldn't this have changed? Why didn't it
7 change? Agent Johnson is Mr. Kurtz's witness at this point.
8 He doesn't want to ask him that question because he knows the
9 answer's not going to be what he likes. And so now it's this
10 attempt to pull the wool over the jury's eyes and do some --
11 some computer examination on a computer that we don't know
12 about.
13   We haven't had a chance to investigate. We don't
14 know what kind of programs are running on there. And -- and
15 at the end of that, the hope is that it comes out different
16 so that way we can impeach what Agent Johnson has already
17 testified to. And there is no reliability in this test.
18 There's no -- pursuant to Rule 403, I would say that this --
19 the probative value of this is so limited that it's
20 outweighed by the prejudicial aspect, which is that these
21 results could be different. If we're trying to ascertain the
22 truth, then we need to get an expert, like one who's sitting
23 on the stand, and ask him what he thinks about this
24 information.
25   MR. KURTZ: Your Honor, I -- I did ask Special Agent

1   Johnson if he knew what the impact would be and he wasn't

2   sure. Not that I was afraid to ask the question. He gave me

3   an honest answer.

4   THE COURT: In my discretion, I'm going to allow --

5   I'm going to allow it, and I also allow the State full reign

6   on cross to address this issue.

7   MR. ZELLINGER: Your Honor, I'd ask that we be

8   allowed to investigate that computer before this examination

9   --

10   THE COURT: If it's --

11   MR. ZELLINGER: -- occurs.

12   THE COURT: -- going to be used, that's another

13   concern that I have.

14   MR. ZELLINGER: And -- and I think we need to -- I

15   mean, my understanding is, before any of these investigations

16   are done, the FBI needs to take that back to a laboratory and

17   investigate the hard drive. So I guess I'd ask for a couple

18   minutes for Agent Johnson to be able to look at that computer

19   and see what's on it before we start this experiment that has

20   -- I'll -- I'll just leave it at that. But I'd ask for some

21   time to be able to look at that computer to determine if

22   there's anything on it that could cause the timestamps to --

23   to go awry.

24   MR. KURTZ: Your Honor, I'll -- I'll go further than

25   that. I'll say I'll -- I'd be happy if Special Agent Johnson

```
 1    has a computer here, I'll go with that one.  He can use Mr.

 2    Zellinger's computer.  Use any computer in this place he

 3    likes.  I'm pretty comfortable with that.  I'm not worried

 4    about the -- I -- I don't have a fixed computer here.  This

 5    isn't mine; it's my mom's.

 6           MR. ZELLINGER: So, Your Honor, at this point we're

 7    using Defendant's counsel's computer, Defendant's mom

 8    counsel's mom's computer to do a test that isn't in a

 9    forensically sound environment, and the probative value of

10    that test is going to exceed the prejudicial value for the

11    jury.  I -- based on those grounds, I would object.  I would

12    just ask for a couple minutes for Agent Johnson to be able to

13    look at this computer.

14           MR. KURTZ: I'm happy for Special Agent Johnson to

15    be able to -- to look at the computer.  I do apologize.

16           THE COURT: The other question I have, too, before I

17    forget, is I don't know anything about the -- does Vista come

18    in different series or volumes or updates, and does that

19    computer have the same Vista program that the IBM ThinkPad

20    has on it?  I mean, these are all relevant questions that I

21    have about this whole process.

22           MR. ZELLINGER: Can I ask questions on voir dire,

23    Your Honor, to clear up some of these issues?

24           THE COURT: Go ahead.

25           MR. ZELLINGER: Mr. Kurtz had an opportunity.
```

VOIR DIRE EXAMINATION

2   BY MR. ZELLINGER:

3   Q.   Agent Johnson, with respect to what you're being

4   asked to formulate, you're being asked to determine why the

5   open hand and closed hand didn't change over time; is that

6   correct?

7   A.   That's my understanding, yes.

8   Q.   Okay. And is it your understanding that JavaScript

9   -- JavaScript controls if the -- if the file is displayed or

10 how it's displayed?

11   A.   It could have an impact on it, yes.

12   Q.   Okay. And that file is not downloaded every time

13 from Google every time you use Google Maps, is that correct?

14   A.   That's correct.

15   Q.   So based on the fact that JavaScript controls it

16 and the file is not created anew every time, what if anything

17 do you hope to get out of this test?

18   A.   I don't -- I'm not trying to get anything out of

19 this test.

20   Q.   Okay. Do you have an opinion as to why the open

21 hand and closed hand reflect July 11th at 1:15 p.m.?

22   A.   Those were the dates and times that they were

23 downloaded and placed on the computer.

24   Q.   Okay. Using Mr. Kurtz's mom's computer, is that

25 going to change your opinion in any way?

A.   No.

         Q.   Okay. Have you ever done a forensic examination or

a test on a computer in a courtroom in front of a jury

before?

         A.   No, I have not.

         Q.   And why does that cause you pause?

         A.   Because it's not a -- a laboratory-controlled

environment. I -- I don't know what's on this computer. I

would like to access, you know, certain information that I

may not have access to here, as far as, you know, clearing up

any questions I may have along the way.

         There is the -- the question of how closely this

specimen would match the original subject machine as far as

its setup, how it would interact with -- I don't know what

service pack is on this one, for example. I know the -- the

subject machine was a -- a Windows Vista Enterprise edition,

with a service pack one. If this is a Windows Vista Home

edition with service pack three, that could potentially

render some of the results a -- a little different.

         And -- but -- but my main concern would be how Google

now translates sending files back and forth to -- to client

machines. I'm just not sure how -- if they would be -- I --

I don't know if it's totally different. I have no reason to

believe that it's different. I do know they did change a lot

of their coding since 2008, since -- since the subject ran --

1 ran his -- his initial test. I -- I just -- but these are

2 the types of things I would rather take a look at in my lab.

3   Q. When you talk about your lab, is it part of your

4 testing to try to be scientifically as exact as possible?

5   A. Absolutely.

6   Q. And do you feel that you can be scientifically

7 exact in this courtroom using that computer you've never

8 looked at before?

9   A. No.

10   MR. ZELLINGER: Nothing further, Your Honor.

11   THE COURT: Any thoughts, Mr. Kurtz?

12   MR. KURTZ: Yes, Your Honor.

13   VOIR DIRE EXAMINATION

14 BY MR. KURTZ:

15   Q. Special Agent Johnson, is there any specific reason

16 to believe that a variation on a Vista OS would have any

17 direct consequence to the file access time under standard

18 information, is there any -- any literature out there to

19 suggest that that would be the case?

20   A. I would have to look for it. Not that I know of,

21 but it doesn't mean that there's not. I --

22   Q. Do you --

23   A. -- I just don't know.

24   Q. -- do you have any reason to believe that it would

25 react differently between OS's, or is this a function of

1 literally when the file is last accessed? And actually, a

 2 better way to ask this: What does file last accessed mean?

 3   A.   It -- it means when the file was last touched on

 4 the computer.

 5   Q.   And what does that mean, when a file is last

 6 touched on the computer?

 7   A.   When it was last accessed by some kind of

 8 interaction. It could be user interaction. It could be

 9 touched by an antivirus program, any number of things.

10   Q.   If you move a cursor from one side of the screen to

11 another and the cursor is -- that's the first time the cursor

12 exists, when you first click on the screen, is that when the

13 create time occurs?

14   A.   That is consistent with the tests that we ran, yes.

15   Q.   And when you let go of the cursor at the end of the

16 navigation, is that consistent with when the last accessed

17 time occurs?

18   A.   Again, it's -- it's my recollection on those tests

19 that -- to answer your question, no. It was the time that we

20 clicked on the -- the left button to close the hand. That

21 was when the file was downloaded and those were the -- those

22 were the consistent dates across the board. So if -- if we -

23 - if we had went back and used that icon again, that closed

24 hand function, it did not update those dates -- or the times.

25 They were all reflected of when they were first initiated.

1   Q.   Do you still have that test data?

2   A.   I'm sure we do. I -- I believe that was a large

3 part of Officer Chappell's testimony.

4   Q.   Is there any -- is -- the test data that resulted

5 from Officer Chappell and your testing, is that particular

6 data in any way a jeopardy to national security if it was

7 disclosed to us?

8   MR. ZELLINGER: Your Honor, I'm going to object.

9 This is far outside the scope of determining whether that

10 computer is proper for an examination. And -- and we're also

11 delving into a -- an issue of law here for the Court and not

12 for Agent Johnson.

13   MR. KURTZ: Well, Judge, there is potentially a

14 piece of information that exists on Mr. Cooper's computer

15 that could say definitely that this material was planted,

16 absolutely definitive. I may be wrong. Special Agent

17 Johnson's testing may indeed be that it all has the exact

18 same millisecond all the way across. I don't think I'm

19 wrong.

20   Now, one way or the other, whether it's having a --

21 a test done on a Vista machine now and seeing what it -- what

22 it actually shows or giving us access to the original test

23 data, which I don't believe has any national security

24 ramifications since it deals with a Google Map test. One way

25 or the other, we should be entitled to this information as it

1 could be tremendously exculpatory.

2   THE COURT: Upon reconsidering this issue about this

3 in-court test, pursuant to Rule 403, I'm going to sustain the

4 objection and exclude any testing in Court because of the

5 differences in the equipment and the statements made by this

6 witness that this is not the appropriate place to do it. We

7 need to bring the jury back in. And regarding the national

8 security issue, that is a matter that we have already ruled

9 on. It is something I have already dealt with.

10   MR. KURTZ: But, Your Honor, there is a witness on

11 the stand that can answer specifically whether this is an

12 issue of national security. And I'm not even going to be

13 allowed to ask that question?

14   THE COURT: I believe I've already determined,

15 because of the rules of the -- and the discovery process that

16 you are not entitled to get those things.

17   MR. KURTZ: So my understanding is, the -- the rules

18 and the discovery process, we're hiding behind national

19 security on an issue where we could get a clear answer from a

20 witness that this is not in fact a national security issue.

21 And we're talking about a piece of information that could be

22 exculpatory to Mr. Cooper.

23   MR. ZELLINGER: Your Honor, first of all, the

24 exculpatory information is already in the Defendant's

25 possession. He has all the files. The fact that his expert

```
 1   is -- his alleged expert can't speak to that is what the
 2   issue is before the Court.  But as to any exculpatory
 3   information, all that has been given to the Defendant.  All
 4   those computer files have been given to the Defendant.  So I
 5   -- I want to just take issue with that and I -- I just wanted
 6   to put that on the record, as to the rest regarding --
 7             MR. KURTZ: Your Honor, that -- that is an
 8   inaccurate statement because we're not talking about data
 9   from this computer.  We're --
10             THE COURT: You're --
11             MR. KURTZ:  -- talking --
12             THE COURT:  -- talking about the pink computer?
13             MR. KURTZ: We're talking about data that Special
14   Agent Johnson and Officer Chappell generated when they
15   attempted to replicate the search.  When they did -- when --
16   replicated this search, they will have generated -- and in
17   fact, we've got a screen shot that shows the first of the
18   timestamps.  There are additional timestamps that are off
19   screen.  Those additional timestamps would answer this
20   question definitely.  And there can be no national security
21   issue here, given we're talking about Mr. Cooper's computer
22   alone and the data that was generated during their testing.
23             THE COURT: It's the methodology that they used, I
24   think, that falls under the security issue, but --
25             MR. KURTZ: But if I could ask Special Agent Johnson
```

if he has any national security concerns related to that
methodology, we might be able to determine that this one
particular test is a legitimate one to be disclosed, that it
will not actually disclose the missile codes.

MR. ZELLINGER: Your Honor, I'm looking at the --
the affidavit of the FBI agent who provided an affidavit to
the Court on June 10th of 2010. And -- and that set out the
FBI current policies and procedures for the viewing,
extraction, and or examination of digital data, the FBI's
policies on the analysis, or -- or how it was -- how it was
examined, numerous other documents from FBI Special Agent
Johnson pertaining to his examination of the computers in
this case, including but not limited to, communications logs,
examiner bench notes, and all other documents completed or
compiled by Special Agent Johnson beyond the report of the
examination.

That's what we're seeking to protect here, because
we don't want, pursuant to state case law, we -- the standard
operating procedures of the FBI are protected throughout our
nation.

And we're not hiding behind anything. All that
information's been given to the Defendant. Agent Johnson's
given out more information in this case than he's ever given
out in any other case. And as to the -- the specific
material that the Defendant wants, he has these files. If --

1 if their exculpatory, take them to an expert and find out how

2 their exculpatory.

3   But the fact is that these files the Defendant has

4 in his possession. Asking Agent Johnson on voir dire about

5 national security just seems wildly inappropriate to me, and

6 then he wants to know exactly how every part of every test

7 that Agent Johnson does can affect national security and that

8 people could be put in danger or child pornography could --

9 could easily be deleted after this information comes out.

10 And we're re-litigating this issue again.

11   MR. KURTZ: Your Honor, what Mr. Zellinger is saying

12 is -- is flat out dishonest and is ascertainable by asking

13 Special Agent Johnson if this is information that we ever

14 got. He's saying we have these files; we don't have these

15 files. These are not the files from Mr. Cooper's computer.

16 These are the files from Special Agent Johnson and Chappell's

17 tests.

18   THE COURT: The objection is sustained. I'm not

19 going to allow further questioning in this line or any in-

20 court testing of that computer. We need to bring in the

21 jury.

22   MR. KURTZ: Your Honor, at this time I am moving for

23 a mistrial and asking for Your Honor to recuse. I believe

24 that your bias throughout this trial has become apparent. I

25 am making this motion pursuant to the Fifth and Sixth

1   Amendments to the U.S. Constitution, the Fourteenth Amendment

2   of the U.S. Constitution, North Carolina State Constitution,

3   Sections 19 and 23. I believe that your rulings have

4   consistently been outside the bounds of prudent

5   jurisprudence.

6   THE COURT: Your objection and motion is noted for

7   the record. Your motion is denied.

8   MR. KURTZ: And as to this particular issue, my

9   inability get potential exculpatory information from Special

10   Agent Johnson's testing, I am also Constitutionalizing that

11   objection pursuant to the Fifth and Sixth Amendments to the

12   United State Constitution, along with the Fourteenth and

13   Sections 19 and 23, Article One of the North Carolina State

14   Constitution.

15   THE COURT: They are noted for the record and

16   overruled. If you'll bring in the jury.

17   MR. ZELLINGER: Before we bring in the jury, can we

18   remove the cables from the --

19   (The jury entered the courtroom.)

20   THE COURT: Welcome back. I see all members of the

21   jury are present. We are ready to proceed. You may resume

22   with your examination.

23   CONTINUED DIRECT EXAMINATION

24   BY MR. KURTZ:

25   Q.   Special Agent Johnson, you -- you have performed

1 testing of separate systems to attempt to replicate the

2 activity that you saw on the IBM ThinkPad, have you not?

3   A.   That's correct.

4   Q.   And in that testing, you did not compare the

5 creation dates, the modification date, and the access date

6 for the cursor files; is that correct?

7   A.   We did, yes.

8   Q.   You recall actually testing those?

9   A.   We -- we compared. We compared the -- the create

10 date from the -- from -- from when we downloaded it to see

11 when it was downloaded.

12   Q.   Did you actually -- well, did you get a standard

13 information entry date?

14   A.   As far as what was displayed in the -- the folder

15 for the -- the temporary internet folder that it was located

16 in, yes.

17   Q.   And was that a valid date?

18   A.   It appeared to be so.

19   Q.   You provided a copy of a master file table that was

20 a fresh install of Vista that you performed?

21   A.   That's correct.

22   Q.   And do you recall -- or actually, I believe it was

23 Officer Chappell, but do you recall Officer Chappell talking

24 about the percentage of files with standard information --

25 well, actually, with invalid timestamps?

```
1    A.   I do.
2    Q.   Do you recall what that percentage was?
3    A.   I believe it was -- for the fresh install, I
4  believe it was like 1.98 percent.
5    Q.   Now --
6    A.   I'm sorry.  No, I believe that was a little over
7  two percent, correct?  I -- believe it was more on the virgin
8  install than it was on the analysis from the subject machine,
9  so I believe that was a little higher than two percent.
10   Q.   Now, the -- on the actual install that -- that was
11 the virgin install, did you count how many invalid time
12 entries existed in different categories, as well as simply
13 overall?
14   A.   I believe we calculated those at the bottom.
15   Q.   And different types of timestamps are actually --
16 serve different purposes.
17        MR. ZELLINGER: Objection to the leading.
18        THE COURT: Overruled.
19   A.   Yes.
20   Q.   Could you explain what standard information entry
21 modified means, what that category of timestamp means.
22   A.   Roughly it is the -- is the last time the dat file
23 was modified.
24   Q.   When you say modified, in what mean -- but how,
25 modified how?
```

1   A.   Again, it's a -- it's a variety of -- it could be a

2   -- a couple different ways. Modified by a -- another

3   program, the user somehow accessing that file again. I've

4   seen -- I've seen those dates get changed from defragging the

5   machine, from antiviruses touching it to see if there's a

6   virus attached to it.

7   Q.   Now, when you and Officer Chappell talked about the

8   total of invalid timestamps, are you referring to -- well,

9   what exactly were you referring to. What number did you give

10 us?

11   A.   Are you talking about the two percent --

12   Q.   Yes, sir.

13   A.   -- that two percent? I believe that was -- that

14 was calculated for all the timestamps across all eight of

15 those columns that the invalid timestamps appeared in.

16   Q.   And when you heard -- when we asked questions about

17 the master file table from Mr. Cooper's computer, which

18 timestamps were included in that number --

19   A.   Which --

20   Q.   -- that was calculated?

21   A.   -- which columns?

22   Q.   Yes, which columns.

23   A.   I believe all of them. I -- I want to say all of

24 them.

25   MR. KURTZ: If I might approach?

1   THE COURT: You may.
         2   Q.   Special Agent Johnson, going to your Vista test, is
         3 that accurate as being the total number of invalid timestamps
         4 across all columns?
         5   A.   Yes.
         6   Q.   Now, if we limit it -- and you're welcomed to
         7 navigate it, if you like --
         8   A.   Thank you.
         9   Q.   If we limit it simply to standard information entry
        10 modified in the virgin install, how many invalid timestamps
        11 are in that category?
        12   A.   Three.
        13   Q.   So three in the complete -- that's the complete
        14 total?
        15   A.   For that column, yes.
        16   Q.   And switching to the standard information entry
        17 date column on your version of Mr. Cooper's ThinkPad, since
        18 it's not totaling --
        19   A.   It's probably down at the bottom. Did you -- did
        20 you reorganize those columns? Were -- were you calculating
        21 them or resorted them?
        22   Q.   I may have resorted them, but one easy way might be
        23 -- no.
        24   A.   Are you working off a CD or a saved copy?
        25   Q.   Saved copy.

```
 1      A.   Did you save it since you re-sorted it?  If you'd -
 2  --
 3      Q.   I don't know.
 4      A.    -- pull it from a backup, it should be the lab
 5  ones.
 6           MR. ZELLINGER: Your Honor, I would object.  Can we
 7  -- I just wonder if we could publish this at this time.  I
 8  wouldn't object to that as to the -- everybody could see what
 9  was going on.
10           THE COURT: I'm going to allow him to proceed as he
11  sees fit.  Overruled.
12           MR. ZELLINGER: Thank you, Your Honor.
13      BY MR. KURTZ:
14      Q.   Do you recall if it was the same number in the --
15  same number of invalid timestamps between your MFT and the
16  MFT that we had provided in the standard information entry
17  modified?
18           THE COURT: What?  They -- they can't hear, so y'all
19  need to speak up.
20      Q.   Do you -- do you recall if the MFT that y'all had
21  pulled had the same number of invalid timestamps as the MFT
22  that we had pulled?
23      A.   I believe they did.
24      Q.   And looking at it from our MFT, filtered by invalid
25  timestamps in the standard information entry date, pulling
```

1 those, how many records did it pull?

2   MR. ZELLINGER: Your Honor, at this point there's

3 been no foundation for the Defendant's MFT report. I'd

4 object to that being utilized for this witness.

5   MR. KURTZ: It's actually been introduced into

6 evidence. I'm sorry?

7   THE COURT: Can you -- Mr. Zellinger ---

8   MR. ZELLINGER: Well, it has been --

9   MR. KURTZ: Sure.

10   MR. ZELLINGER: -- identified. I don't believe the

11 Defendant's MFT has been introduced into evidence.

12   MR. KURTZ: It has actually been introduced into

13 evidence. This was pursuant to an argument about the entire

14 computer having been introduced.

15   THE COURT: Can you tell me -- I'm going to allow it

16 because I do believe it was at least published to the jury on

17 the screen, because I remember the -- are we talking about --

18   MR. KURTZ: It's Defendant's 115, Your Honor.

19   MR. ZELLINGER: Your Honor, the argument that was --

20 that it was admitted as State's 305, which is the actual

21 laptop. If that's how we're operating, I'll withdraw my

22 objection, but that's to indicate that anything on that

23 computer is admissible.

24   THE COURT: I'm going to allow him to proceed. Go

25 ahead.

```
 1              MR. ZELLINGER: But -- but, Judge --

 2              THE COURT: The objection's overruled.  Go ahead.

 3       BY MR. KURTZ:

 4       Q.    Okay.  Special Agent Johnson, showing you the MFT

 5   that was extracted by the defense, and I've sorted it, or

 6   filtered it, more appropriately, just to show how that was

 7   done.  The only selections are the invalid timestamps, and

 8   are you able to determine how many invalid timestamps it

 9   appears to contain?

10       A.    No.  Oh, you're talking about the -- down here, the

11   3,349.

12       Q.    Okay.  And that's actually just the standard

13   information entry date.  When the numbers were compared

14   between the two computers, the three -- the two-and-change

15   percent for your extraction, that was for all eight fields?

16       A.    Yes, sir.

17       Q.    And for the Defense, the 3,349 were simply for the

18   standard information entry modified category, correct?

19       A.    I believe there were -- I believe there may have

20   been four -- four or five other invalid timestamps in the

21   file name attribute column for the very first one -- I forget

22   which one that is, created maybe?  I believe there were a few

23   more, but a very small number.

24       Q.    Is there any certification for being an expert on

25   internet history files?
```

```
 1      A.    Are you talking about analyzing internet history

 2   files?

 3      Q.    Correct.

 4      A.    Not that I'm aware of.  Although there are classes

 5   that are specific to internet artifacts.

 6      Q.    And are any files between July 11th and July 15th

 7   deleted that were significant that you were able to

 8   determine?

 9      A.    That I was able to extract for --

10      Q.    Yes.

11      A.     -- for that day branch?

12      Q.    Yes.

13      A.    Without looking at my report, I would have to say

14   no, but none -- none that I recall, so probably not if

15   they're not standing out in my mind.

16      Q.    If in your test results there was a different

17   modified time from create time of a cursor, would that

18   potentially impact your opinion related to the information on

19   Mr. Cooper's machine?

20      A.    At -- at the outset, I would say probably -- I

21   would say no, but I would -- I would have to do more analysis

22   on that, if -- if that's what I found.

23      Q.    And --

24      A.    If I'm understanding your question.

25      Q.     -- how would you actually -- what kind of testing
```

1 would you perform to attempt to make that determination?

2   A.   Are you saying if the -- if the open cursor file

3 had a different access date -- access create date versus a

4 modified create date, right?

5   Q.   Yes, sir.

6   A.   The first thing I would do would be to try to

7 contact, you know, a programmer at Google to see how exactly

8 those files are interacting, when they're interacting, if

9 there is a difference on OS version on how those are -- are -

10 - are handled on a -- on a specific computer. That's the

11 first thing I would do, to see if there's some kind of a

12 programmer reason as to why those are -- are changing.

13   Q.   Okay. There were Google cookie -- were there

14 Google cookies at all on Mr. Cooper's machine?

15   A.   Yes.

16   Q.   Were there any Google cookies at all that spanned

17 July 11th?

18   A.   Not that I recall.

19   Q.   Do Google cookies contain unique information that

20 allow you to -- allows you to get a court order?

21   A.   Again, I remember you asking me this the first

22 cross. They -- they could, but again, I would -- I would

23 want a little bit more than that.

24   Q.   What do you mean by you would want a little more

25 than that?

1   A.   I would want to see some more files, other than

2   just a cookie file.

3   Q.   Is there a reason why that neither you nor Officer

4   Chappell requested cookie information from Google in this

5   case?

6   A.   Yeah. It's -- it's really -- it really wasn't our

7   -- it really wasn't our duty or responsibility to -- to do

8   that. I mean, as an examiner, I can't -- I can't issue

9   subpoenas based on investigation or, you know, write a court

10   order. I can advise the primary investigator to do that,

11   which -- which we did.

12   Q.   Who did you advise?

13   A.   I believe it was Officer Young.

14   Q.   And what did you advise him to do?

15   A.   That he needed to probably contact Google and see

16   about their logs for that time frame.

17   Q.   And what was his response?

18   A.   It was something like, "I'll take that under

19   advisement." I mean, I never -- we never heard back on that

20   issue.

21   Q.   Had that been done, what kind of information would

22   you expect you could have gotten from Google?

23   MR. ZELLINGER: Your Honor, I'd object to the

24   speculation.

25   THE COURT: Overruled, if he knows.

1   A.   Typically, we'd receive log information back from

2 Google, which would specify the date, time, IP address that

3 connected to their servers at that date and time, indicating

4 that connection and information was exchanged.

5   Q.   So that would be pretty hard evidence?

6   MR. ZELLINGER: Objection, Your Honor.

7   THE COURT: Sustained as to the form of that

8 question.

9   BY MR. KURTZ:

10   Q.   Would that be -- would that be external

11 verification if you were to get that kind of information?

12   A.   You would have to -- you have to then match those -

13 - that information up with the Cisco logs because that would

14 not -- it -- it would -- I would expect that would come back

15 to a Cisco IP address connected with our Google servers at

16 that date and time. That's all that Google would be able to

17 tell you is that, yes, someone from -- from the Cisco system

18 accessed our servers. From that information, you would have

19 to then go to Cisco to obtain that information from them to

20 try to ferret down which computer that came from.

21   Q.   But am I correct that it -- it would tell you

22 exactly what time a search took place, wouldn't it?

23   A.   Depending on when you got that information back and

24 assuming that both Google and Cisco would still have those

25 logs, I would expect you would be able to -- to track that

1 down, yes.

2   Q.   Now, you say that that was something that you had

3 recommended to Detective Young, but in other situations in

4 this case, you requested information from Google, didn't you?

5   A.   No, that's incorrect. All I did was fax out a

6 preservation request. That's -- that's not requesting

7 information from them. I'm just requesting that they do not

8 erase or -- or -- or -- or extinguish or purge information

9 from a certain time frame or associated with a certain email

10 address. I believe you're referring to the -- the BB simple

11 --

12   Q.   Uh-huh.

13   A.   -- email address. They will not give me any

14 information based on that letter. All they'll do is they'll

15 pull that aside for, I think, a span of 30, 60 days to give

16 me or an investigator time to get a court order or a subpoena

17 out to them.

18   Q.   Is there a reason why you didn't do the same sort

19 of preservation letter for potential Google cookie

20 information?

21   A.   I would -- I would surmise that the reason I did

22 that initially was because Cary P.D. was not aware of that,

23 and so they probably requested that I send that out and it

24 was just easier for me to do it myself than explain to them

25 how to do it, explain to them the verbiage. I've done that

1 multiple times before as -- as an investigator.

2   Again, I'm just surmising that, once I showed them how

3 to do it the first time, I assumed that they would probably

4 know how to do it for any other -- any other additional

5 information that they would need from Google or any other

6 company with such logs. But that's -- that's just a guess.

7   Q.   Have you -- what are the possible causes for there

8 not to have been any cookie on Mr. Cooper's machine for July

9 11th?

10   MR. ZELLINGER: Objection.

11   THE COURT: Overruled, if he knows.

12   A.   One possible explanation is that -- and again, I

13 would have to go -- I was reading about it the other day, and

14 I would have to go -- I'd have to go reference my -- my

15 materials -- but there was something to do with the cookies

16 being associated with the RAM and that it may have been kept

17 in the RAM area of the -- of the machine. And, basically,

18 once that computer goes down, anything in the RAM is -- is

19 deleted. But again, that -- that's just a loose, very quick

20 explanation. That was -- that was one explanation that we

21 could -- that we found that -- that the way Google operates

22 some of those cookies.

23   Q.   Where did you find the other Google cookies that

24 were on his machine?

25   A.   They were in the cookie file.

1   Q.   So there is actually a folder where they're kept?

2   A.   Yes, sir.

3   Q.   And did you search for deleted --

4   A.   I did.

5   Q.   -- cookies? And were there any remnants of

6 deleted cookies from that time?

7   A.   No, there were not.

8   Q.   Was there any -- was there any evidence on the

9 machine that cookies had been deleted and then purged in some

10 fashion?

11   A.   Not that I saw.

12   Q.   How -- in your opinion, how would a -- a forensic

13 expert analyze internet history files differently from a

14 network security expert?

15   MR. ZELLINGER: Your Honor, I'd object to the form

16 of that question.

17   THE COURT: Overruled, if he knows.

18   A.   Being that I'm not a network security expert, I --

19 I -- I wouldn't -- I wouldn't know. I just know what I would

20 do as a forensic examiner.

21   MR. KURTZ: May I approach the witness, Your Honor?

22   THE COURT: Yes, sir.

23   BY MR. KURTZ:

24   Q.   Special Agent Johnson, I'm showing you what's been

25 marked as Defendant's Exhibit 117. Is that an accurate

```
1   representation of the cookies that you did find on Mr.

2   Cooper's system -- the Google cookies, specifically?

3       A.   I don't remember dates and times for those

4   individual cookies.  I also don't -- I don't recall the G

5   modules, but the number sequences seem to be correct.

6       Q.   And so do you -- you recall that all of the cookies

7   that existed prior to the 11th actually terminate on the

8   10th?

9       A.   Is that on here?

10      Q.   I'm thinking it's there, but I'm not sure.

11      A.   Is this your termination point right here?

12      Q.   It is.

13      A.   These all -- these all say --

14           THE COURT: Speak up louder so that --

15           THE WITNESS: Oh, I'm sorry.  I'm sorry.

16      A.   These all indicate the 2008th -- 2008 on July 6th.

17      Q.   Those all terminate on July 6?

18      A.   According to this graph, yes, sir.

19      Q.   And then when do they restart?

20      A.   They don't appear to restart, unless you're

21   referring to --

22      Q.   Yes, sir.

23      A.    -- these over here.  July 15th.

24           MR. ZELLINGER: Your Honor, I'd object at this point

25   to -- just to be clear, this is what's on this document.
```

1   There's been no foundation for where these numbers came from.

2   THE COURT: Can you provide a foundation for that or

3 -- I don't know. I mean, he can testify about them -- he's

4 talked about them somewhat, but I don't know if he has

5 independent knowledge of them or enough recollection about

6 them to speak about them at this point. But, I mean, if you

7 can go -- go ahead.

8   MR. ZELLINGER: I'll withdraw my objections.

9   BY MR. KURTZ:

10   Q.   Would the net analysis report that you did assist

11 in determining whether those are accurate?

12   A.   Yes.

13   Q.   Do you recognize those as being the net analysis

14 files?

15   A.   Yes.

16   Q.   Is one -- would one of these be better for you to

17 look at than the others?

18   THE COURT: Can you speak up just -- I want to make

19 sure that they hear you.

20   MR. KURTZ: Yes, sir, sorry.

21   A.   Not necessarily, probably the first one.

22   MR. ZELLINGER: Your Honor, may I approach and just

23 see what --

24   THE COURT: You may.

25   BY MR. KURTZ:

Q. Is that a report that would assist you in determining whether or not those cookies match up?

A. Yes.

THE COURT: I think this would be a good time for us to take our afternoon break while he's doing this. Members of the jury, I'm going to release you for a 15-minute recess and ask you to return to the jury room at 20 till three. Please keep in mind the rules, that is you cannot talk about the case. Don't let anybody talk about it in your presence. Don't form any opinions. Don't conduct any independent research or investigation. Don't concern yourself with any new accounts. Please return to the jury room at 20 minutes 'til 3. I'm going to ask everyone else to remain seated in the courtroom.

(The jury left the courtroom.)

THE COURT: Let the record reflect that all members of the jury have left the courtroom. We'll be at recess for 14 minutes.

(The Court recessed from 2:26 p.m. to 2:40 p.m.)

(The Assistant District Attorneys, Counsel for Defendant, and the Defendant were present in the courtroom. No jurors were present.)

THE COURT: Let the record reflect the Defendant's present with his attorneys as well as Counsel for the State. Anything for the State before we resume?

1   MR. ZELLINGER: No.

2   THE COURT: Or the Defense?

3   MR. KURTZ: No, Your Honor.

4   THE COURT: Do you need additional time with this

5   witness --

6   MR. KURTZ: To go over --

7   THE COURT: -- over that line of questioning or

8   does he --

9   MR. KURTZ: No, we're going to move forward.

10   THE COURT: All right. If you'll bring in the jury,

11   please.

12   THE COURT OFFICER: Yes, sir.

13   (The jury entered the courtroom.)

14   THE COURT: All right. I see all members of the

15   jury are present. We are ready to proceed. You may resume

16   with your examination.

17   MR. KURTZ: Your Honor, at this time I'd like to

18   publish Defendant's 118 to the jury.

19   THE COURT: You may.

20   MR. ZELLINGER: Your Honor, I would object again in

21   that, at the time that this was admitted into evidence, we

22   were in a different position than we are today.

23   THE COURT: Overruled.

24   MR. ZELLINGER: And that the -- as to who created

25   Defendant's Exhibit 118.

```
 1              THE COURT: I'm going to allow him to publish it if
 2    this witness can testify as to the basic foundational matters
 3    and if it is illustrative of his testimony.
 4         BY MR. KURTZ:
 5         Q.   Okay.  Special Agent Johnson, does Defendant's
 6    Exhibit 118, did --
 7              MR. ZELLINGER: I'm sorry Your Honor, I withdraw
 8    that.  I -- I thought -- I was looking at a different
 9    exhibit.  I withdraw that for 118.
10              THE COURT: Okay.
11              MR. ZELLINGER: I apologize.  It's my fault.
12              THE COURT: Let's go ahead and publish it.
13              MR. KURTZ: Okay.
14              THE COURT: Is that what you're saying?
15              MR. ZELLINGER: Yes, yes.
16              THE COURT: Okay.
17              MR. ZELLINGER: That's my fault.  That was just 118,
18    Your Honor?
19              MR. KURTZ: It is 118.
20              THE COURT: Yes.
21              MR. ZELLINGER: All right.  Thank you.
22              (Defendant's Exhibit 118 is published to the jury.)
23              MR. KURTZ: And, Your Honor, while the jury is
24    looking at that, may I approach the witness?
25              THE COURT: Yes, sir, you may.
```

BY MR. KURTZ:

         Q.   Special Agent Johnson, do you recognize that screen
shot?

         A.   Yes.

         Q.   And is that actually the screen shot that you took
doing -- when you were attempting to replicate the Google Map
search?

         A.   Yes, it is.

         Q.   And when was it that you actually performed that
test?

         A.   It appears to be September 15th.

         Q.   So that would've been roughly 90 days after Ms.
Cooper went missing --

         A.   No, I think it --

         Q.   -- or 60 days, sorry.

         A.   Sixty days, yes.

         Q.   Sixty days. Now, the file in 118 shows as being --
which the jury actually has -- shows this being open hand and
closehand1.BMP. How is it displayed in your test results?

         A.   This one says openhand.CUR.

         Q.   Now, do you know the difference between a .CUR and
a .BMP file?

         A.   I'm not -- I know what a .BMP file is. I'm not --
I don't have a lot of knowledge with the CUR, which I'm
assuming stands for cursor.

```
 1        Q.   Is there a reason why BMP files are less common in

 2   internet applications than other type of graphics files, or

 3   is that an accurate statement, is the first question?

 4        A.   They are -- they're an older type of a -- of a

 5   image type file, and people have moved away from them because

 6   they're not as robust or as clear, crisp.

 7        Q.   They're also kind of big files, aren't they?

 8        A.   They are big files.  They're bigger.

 9        Q.   They take up more space?

10        A.   Yes, sir.

11        Q.   And so when you did the test, the file that you

12   rendered resulted in a .CUR?  The one of Mr. Cooper's though,

13   shows as a BMP.  What would account for that difference in

14   file type?

15        A.   First of all, I would have to open this file up to

16   see what it looks like, because I would expect to see -- when

17   I open up a BMP file, I will actually see this BMP image, and

18   I'm not sure if this is the same file.  That would be my --

19   my best guess.  If it is the same file, I -- I don't have an

20   explanation for that.  Maybe between the time, from July to

21   September, they -- they may have replaced that.

22             THE COURT: Meaning they, be who?

23        A.   I'm sorry, Google may have replaced the -- the .BMP

24   with a .CUR, possibly for the reasons that you just cited.

25        Q.   Okay.  And --
```

1   A.   I would have to look.

2   MR. KURTZ: And Your Honor, I'd ask to admit

3   Defendant's 124, which is the screen shot from FBI testing.

4   THE COURT: Any objections to this submission?

5   MR. ZELLINGER: No objection, Your Honor.

6   THE COURT: It's admitted.

7   MR. KURTZ: I'd ask to publish that to the jury at

8   this time, Your Honor.

9   THE COURT: Electronically, or do you want to do it

10   --

11   MR. KURTZ: On paper.

12   THE COURT: All right, you may.

13   (Defendant's Exhibit 124 was published to the

14   jury.)

15   BY MR. KURTZ:

16   Q.   Now, Special Agent Johnson, the -- the different --

17   the first difference that you'd note between the two files is

18   the extension; is that accurate?

19   A.   That is correct.

20   Q.   The create time of the open hand from the IBM

21   ThinkPad, does that correspond, roughly, to the beginning of

22   the sequence of files that you see related to the map search?

23   A.   Roughly at the beginning, yes. I -- I -- I don't

24   remember the exact time, but I believe it was -- this was

25   towards the beginning.

1   MR. KURTZ: May I approach the witness, Your Honor?

2   THE COURT: You may.

3   Q.   Okay. Special Agent Johnson, I'm showing you

4 what's been marked as Defendant's Exhibits 108 through 113.

5 If you could look through those, do they appear to you to be

6 the assembled tiles at various levels of magnification from

7 the IBM ThinkPad?

8   A.   (The Witness examines the exhibit.) Yes.

9   Q.   And, based on that, approximately how many levels

10 of zoom or complete refreshes took place?

11   MR. ZELLINGER: Objection, Your Honor. There is no

12 foundation for those -- well, I'd say that mischaracterized

13 that. And so I also object to the fact that the -- just

14 because there's pictures that Agent Johnson's looking at -- I

15 guess the -- I'm confused as to whether the question applies

16 to how many levels of zoom do you see in the pictures that

17 are in front of him, or how many did he see when he examined

18 the Defendant's computer?

19   THE COURT: If he can tell from the exhibit, I'm

20 going to allow him to answer the question. Overruled.

21   A.   I -- I can't tell by looking at the picture, but --

22 I mean, I can't tell what the zoom level is by looking at a

23 picture.

24   Q.   Are you able to tell how many separate actions took

25 place --

1   A.   From here to here?

2   Q.   -- or a minimum number of actions that took place

3   from the first image to the last image.

4   A.   Approximately six.

5   Q.   And those six actions would have occurred within

6   the 41-second span?

7   A.   Yes.

8   MR. ZELLINGER: Objection, Your Honor. Again, are

9   we talking about the pictures, or we're talking about what

10 was actually on the Defendant's computer?

11   THE COURT: Overruled.

12   BY MR. KURTZ:

13   Q.   At each stage, would -- would an action actually

14 put a cursor somewhere on the screen?

15   A.   Only if the -- you're talking about the open hand

16 cursor -- the -- the -- the Google cursor?

17   Q.   Either -- oh, yes, the Google -- either the open or

18 closed hand.

19   A.   No.

20   Q.   Okay. How -- for what purposes would you see an

21 open or closed Google hand cursor?

22   A.   I -- whenever the -- the Google hand is being

23 manipulated to -- to grab something and -- and to drag.

24   Q.   Okay. From these photos, are you able to determine

25 if the image was dragged at all?

1   A.   From these images, I can't tell, but I -- it would

     2 -- it would be my opinion that they were.

     3   Q.   Okay. And are these fair and accurate

     4 representations of the different stages of tiles from the

     5 internet history folders?

     6   A.   From my memory, they -- they appear to be accurate

     7 representations.

     8   Q.   Thank you.

     9   MR. KURTZ: Your Honor, I ask to admit Defense

    10 Exhibits 108 through 113.

    11   THE COURT: Any objections?

    12   MR. ZELLINGER: I do. I object, Your Honor, in that

    13 we don't know who put these -- these pictures together.

    14   THE COURT: I'm going to allow them. It's up to the

    15 jury to determine the weight of any evidence.

    16   MR. KURTZ: And Your Honor, I'd ask to publish these

    17 to the jury at this time.

    18   THE COURT: You may.

    19   MR. KURTZ: Thank you.

    20   (Defendant's Exhibit Numbers 108 through 113 were

    21 published to the jury.)

    22   BY MR. KURTZ:

    23   Q.   Now, Special Agent Johnson, could you describe the

    24 difference between a regular -- well, where modification date

    25 comes from on a -- an internet artifact?

1   A.   Modified typically -- typically means that

2 something in the file has been modified. I would expect to

3 see that if, for example, I saved a Word document to the

4 computer and then, at a later date, I go in and -- and -- and

5 change something on that -- on that file.

6   Q.   When talking about something that's -- that's

7 internet-based, downloaded internet content, is there ever a

8 situation where the modified time and date is actually the

9 time that it's modified at the server?

10   A.   At the server?

11   Q.   Before it gets to the local machine.

12   A.   I'm -- I'm not sure what you're asking.

13   Q.   Are there times when the modified date will reflect

14 the time that it was last modified by Google, for example?

15   A.   It -- it could. I can't give you an example, but

16 it could.

17   Q.   And what action is required to trigger a time to

18 reset for last accessed?

19   A.   A time to trigger the last access. So what -- what

20 would -- what would modify that column is what you're asking,

21 what --

22   Q.   What --

23   A.   -- would change it or --

24   Q.   What determines that last accessed time?

25   A.   The last time the file was accessed.

1   Q.   Right.   Oh, I'm sorry, I thought you were asking if

2   that was my question.   When you say the last time the file

3   was accessed, what -- what does that really mean?   I mean,

4   how are files accessed?

5   A.   Well, again, those would be the -- I would -- I

6   have seen files get modified under that column after they're

7   accessed by -- by the user manipulating them with some kind

8   of a -- like accessing in through a program, or accessing

9   them just raw on the machine.   I've seen defraggers change

10   that date and timestamp, you know, the anti-virus, anything

11   that touches the -- the file.

12   Q.   And would you expect if an antivirus or defrag had

13   changed the timestamp, that all files that were hit at the

14   same time would be, roughly, close in time?

15   A.   Roughly, yes.

16   Q.   There's nothing about the files that we're looking

17   at -- those being the open and closed hand cursor -- that

18   would indicate to you that there was some sort of defrag or

19   antivirus changing that time?

20   A.   No.

21   Q.   It does appear that there is at least some

22   interaction with the cursor, required by the user, to go

23   between the different -- the different photos -- the --

24   MR. ZELLINGER: Objection.

25   Q.   -- different levels --

```
1          MR. ZELLINGER: Leading.

2      Q.     -- of map?

3          THE COURT: I believe he's already testified to that

4  --

5          MR. ZELLINGER: Asked and answered, Your Honor.

6          THE COURT: In -- he said, in his opinion, something

7  to that effect.  And so as far as leading him, I'm allowing

8  it in this instance.  Go ahead.

9          MR. KURTZ: I'm not sure if that was sustained.

10          THE COURT: No, no.  I'm allowing -- I'm allowing

11  you to -- yes, it was a leading question, but he's already

12  answered the leading question that you asked.  A few minutes

13  ago, he -- he answered a question that he prefaced with "in

14  my opinion," which I believe was related to the question you

15  just asked him, so in this limited basis, I'm going to allow

16  it.  Go ahead.

17      BY MR. KURTZ:

18      Q.    And yet, no matter how slight an action would be on

19  a computer, some period of time would be expected to elapse

20  for it to take place, would it not?  Movement of a cursor,

21  for example.

22      A.    Yes, I mean, if that would take some kind of --

23  some amount of time to --

24      Q.    Some amount of time?

25      A.    Yes.
```

1   Q.   There is no time reflected as being elapsed, from

2   the create time through the access time, on either the open

3   hand or closed hand cursor; is that correct?

4   A.   That's correct.

5   Q.   If you were to place files from a hard drive onto

6   another computer, is there a higher likelihood of all file

7   timestamps being identical?

8   MR. ZELLINGER: Objection to the form of the

9   question and the fact that he's leading.

10   THE COURT: Overruled. He can answer it, if he

11   knows.

12   A.   Can you rephrase that?

13   Q.   Sure. If --

14   A.   I -- I understand you're taking from one -- from

15   one hard drive to another.

16   Q.   Correct.

17   A.   Okay. And you want to know about the --

18   Q.   At that time that they're manipulated, is it

19   possible that all file timestamps, at that point, reset when

20   moved from point A to point B?

21   A.   They -- it is possible for them to reset.

22   Q.   Is it also possible that there are programs that

23   would allow you to predetermine a time for all -- for all of

24   the timestamps to reflect, if you were to move things from

25   one drive to another?

1   A.   I'm not familiar with any such programs, but it

2 wouldn't be -- it would be possible to do that, yes.

3   Q.   And is it possible that moving files from one drive

4 to another could result in an invalid timestamp in the system

5 information attribute entry modified column, in specific?

6   A.   It could.

7   Q.   Thank you.

8   MR. KURTZ: I've nothing further.