MR. KURTZ: Thank you, Your Honor.

CROSS-EXAMINATION

BY MR. KURTZ:

Q. Good afternoon, Officer Chappell.

A. Good afternoon.

Q. Officer, is it safe to say that Special Agent Johnson was the primary forensic examiner in this case?

A. Yes, sir.

Q. He is actually more experienced examiner than you?

A. Yes, sir.

Q. Knows more about computers than you do?

A. Subjective opinion.

Q. You wrote a report that was un' -- it did not bear your name, titled "Refuting the claim of evidence tampering"?

A. Yes, sir. And I wouldn't really characterize that as a report. It was made the night before a meeting just as something to talk about.

Q. It's six pages long, correct?

A. Yes, sir.

Q. And in it you address different -- different scenarios that you believe we were asserting as the way that the computer was tampered with?

A. I think that's accurate.

Q. In your report -- well, how would you categorize it?

A. I think that's accurate, the way you categorized it.

Q. As a report?

A. Semantics, sir. I'm happy to call it a report if that would make this go along.

Q. Okay. In this -- in this report, you actually address a number of issues. One of them is the question of Mac filtering, correct?

A. I believe it was in the context of if Mac filtering were enabled for a wireless access point, that's an additional access of security for the access point.

Q. Right. At the time that -- when did you write this?

A. I don't remember without looking back at a calendar.

Q. Are we talking about something that you wrote in this month? We're at April 13th. Did you write it in April?

A. No. I think it was last month.

Q. Okay. And you were here for Special Agent Johnson's testimony?

A. Yesterday, yes, sir.

Q. At the time that you wrote this, weren't you aware that Mac filtering was not enabled on the Cooper home network?

A. No, sir.

Q. How is it that that is something that Special Agent Johnson were aware of that you were not?

A. I think probably just mistaken.

Q. Did you discuss this report with him before actually presenting it?

A. I don't know that we really discussed the report. I mean, these were topics of conversation that we had.

Q. Did you discuss your testimony today with him after court yesterday?

A. Discuss my testimony for today, no.

Q. You go on in your report to talk about how a master file table of a computer would show if something was out of order.

A. There could be signs that would indicate that, yes, sir.

Q. In fact, Microsoft Windows does not work in a sequential file system, does it?

A. No, it doesn't.

Q. It works in a parent file with sub folders?

A. Well, I think that's an element of it, yes, sir.

Q. And so it -- it's not like things are numbered one to a hundred thousand?

A. There's not like there's an I-note, like in a UNIX file system, no, sir.

Q. So something that is moved from number 70 to number 30 is not necessarily going to be reflected as having been moved that way?

A. Well, the master file table, their entries, entries can be reused. When it gets reused, it gets a sequence number that gets incremented. So if I see something that has a sequence number that's not been incremented, I can conclude that's the first content master file that entry was made. If I see it's 65,000, I can conclude that's been reused a number of times.

Q. But you can't necessarily determine if a particular file has been moved within the master file table unless it happens to be placed in a strange location like that.

A. Just by looking at the master file table, no, sir.

Q. At what point did you actually get a master file table from this computer?

A. When you say get the file table.

Q. Well, it requires extraction, doesn't it?

A. It does.

Q. How do you do that?

A. There's a number of different ways you can do it. We just exported the file table.

Q. How did you export the file table?

A. From within FTK.

Q. Okay. When you exported the file table -- when was it that you exported the file table from FTK?

A. It -- it would have been just prior to that -- that document being written, several weeks ago.

Q. And when you exported that file table, you actually concluded or included in that document was the fourth timestamp field, which is time entry modified, correct?

A. Well, the master file table, it's called the entry update. So it would be the time that the master file table file name entry should have been updated.

Q. But I'm not actually talking about the file name section, I'm talking about standard information attributes.

A. Yes, sir, but that standard information attribute column, it should relate to the time that the file name attribute column was updated.

Q. And that is the fourth timestamp value, correct?

A. Entry update.

Q. When you actually wrote this report, you had already extracted that information, correct?

A. Extracted the master file table, yes, sir.

Q. And after looking at the master file table, you became aware that there were a number of files that said invalid timestamp in the -- within the entry modified category?

A. There were several, yes, sir.

Q. And that's not something that you noted in your report anywhere?

A. No, sir.

Q. Did you at that time note that prior to July 8th, there were fewer than 20 invalid timestamps on that computer?

A. No, sir. I think what you're referring to is probably a report that I did not do, so I -- I wouldn't -- I wouldn't be able to characterize that.

Q. Well, I'm referring to your report, Officer. And in that, you don't actually note any invalid timestamps anywhere in it.

A. That's correct.

Q. My question about when you wrote your report is did you -- is that something you omitted intentionally when writing the report?

A. Well, I don't know that I reflected a lot of things that I didn't feel were relevant to my report.

Q. In --

A. I didn't include negative findings, if that's what you're asking.

Q. The search that we've been talking about, the search on the map for Fielding Drive from start to finish, that's a 41-second duration of time; is that accurate?

A. Yes, sir.

Q. In that 41 seconds, I believe it's 507 files that are created?

A. I'll take your word for it. I don't know without looking at the -- the output from FTK.

Q. Did you look to even see that all 507 of the files bear invalid timestamps?

A. Invalid in the single category out of the eight timestamps?

Q. Yes, sir.

A. No, I did not.

Q. On the entire computer, how many files had invalid timestamps overall?

A. Invalid in that single column or invalid in any standard information or file name attribute column?

Q. Well, for the moment, in entry modified, since that's what we're talking about.

A. I do not know.

Q. Why don't you?

A. Because I did not do an exhaustive count of invalid timestamps in that particular column.

Q. Well, you knew that there was an accusation of tampering with the computer.

A. Yes, sir.

Q. And you actually wrote a report refuting that claim.

A. That's correct.

Q. And you determined it wasn't worth following up on an invalid timestamp entry?

A. That's one element of multiple elements on that computer. And that element could be explained as simple as the particular tool that I used wasn't interpreting that data correctly. I found that the standard information attribute, the other three values were all consistent with the file name modification and creation times. And the file name attributes are very difficult to tamper with. And since there were no invalid entries in those file name attributes, I concluded, based on my experience and training, that that could be a tool interpretation issue.

Q. But you'd seen our expert's report, as well?

A. Yes.

Q. And in fact, those findings corroborated yours, in that his extraction of the master file table produced the same invalid timestamp result that you saw?

A. Well, I would categorize that as a tool he used produced results that were replicated by the tool that I used. In, you know, there's multiple ways of doing that. I can't test it with every single tool. But I was satisfied, based on the other seven timestamp values, that there was no tampering with a particular set of files.

Q. But in fact, both of those tools did render the same result as them being invalid?

A. If you use the same tool, you should get the same results.

Q. Do you know that you used the same tool as Mr. Ward?

A. He referenced something called CAINE. It's a forensic linux distribution. It's Italian.

Q. It's a different tool than what you used, isn't it?

A. To evaluate the timestamps?

Q. To extract them.

A. Well, to extract them is one thing, but to evaluate the timestamps, I mean, exporting a master file table doesn't give me the timestamps. I have to run a tool in order to extract that data from the master file table.

Q. You're saying that the same tool ran twice gave the same results; in fact, saying that it was done the same way. You don't know that the way you did it is the exact same way that Mr. Ward did it?

A. No. I was basing it on what he said in his report.

THE COURT: Just a second. In my discretion, I'm going to take a brief recess, and I'm going to ask members of the jury to step to the jury room. And once you all are in a position, if you'll knock on the door and let Mr. Liles know that -- what your status or progress update is.

(Jury exits the courtroom at 3:44 p.m.)

THE COURT: The jurors have handed Mr. Liles a note which they've indicated that one of the jurors is having some health issues, and they wanted to take a break and she would would need some time. So we're going to need to be at ease until we hear something back from them. It would be my intent to give them 10 or 15 minutes if they haven't knocked by then.

We'll just be at ease. If they knock before 4:00, let me know.

THE DEPUTY: Yes, sir.

THE COURT: Otherwise we may need to inquire whether she'll be in a position to proceed today.

Yes, sir. We'll be at ease until they knock or 4:00, whichever comes first.

(Court at ease.)

THE COURT: If you'll bring in the jury, please.

(Jury enters the courtroom at 4:03 p.m.)

THE COURT: Welcome back, members of the jury. In my discretion, I'm going to release you. It's 4:00, a couple minutes after 4 now. I'm going to release you and ask you to return tomorrow morning at 9:30 a.m.

Just -- I'm going to -- you know I'm going to remind you about the rules. Be very careful about your conduct. Be careful that you don't talk about this case among yourselves or allow anybody to talk about it in your presence. Don't concern yourself with any media accounts that may be out there, and you're not to conduct any type of independent research or investigation.

You all have got a copy of those rules, I gave them to you at the very beginning. I hope that you still have it. There are two phone numbers on there, I'll just remind you that. If you need to report to us in the morning or for whatever reason if you don't have the numbers handy, tear a page out of your book right now and I'll let you write it down. It's 792-4406, and that's Sonya in the clerk's office downstairs. And if you need to convey any message to us, you may do so in the morning.

That is your jury room. You are free to use it as long as you need to use it this afternoon. If you need to stay up here for a few minutes, that's fine. I'll need to close the door and the sheriffs are also here to assist you in any way.

With that being said, I'm going to ask everyone to remain seated while the jury is excused until 9:30 a.m. tomorrow morning.

(Jury exits the courtroom at 4:05 p.m.)

THE COURT: Let the record reflect that all members of the jury have left the courtroom.

Is there anything on behalf of the State or the defense before we adjourn?

MR. ZELLINGER: No, Your Honor.

MR. KURTZ: Your Honor, I would request, since we happen to have overnight, to get a copy of the master file table, just require burning onto a CD.

MR. ZELLINGER: Can I speak with counsel afterwards, and I'll try to help him with whatever he needs?

THE COURT: I don't have any idea what all that entails, but if you all can work it out, that would be great. We'll be at recess until 9:30.

Did you have anything else?

MR. KURTZ: No, Your Honor.

THE COURT: Thank you. Be at recess until 9:30.

(End of day's proceedings.)

THE COURT OFFICER: Yes, Your Honor.

(The jury entered the courtroom.)

THE COURT: Good morning. I see all members of the jury are present and ready to proceed. If you'll take a moment to make sure that we got the right notebooks into the right chair. And once again, I'll remind everybody that all cell phones and electronic communication devices need to be turned off. That applies to those in the gallery. And, Mr. Kurtz, you may resume your examination.

MR. KURTZ: Thank you, Your Honor.

CONTINUED CROSS EXAMINATION

BY MR. KURTZ:

Q. Good morning Officer Chappell.

A. Good morning.

Q. Officer, I -- I'm afraid I'm not positive exactly where we left off yesterday, so I'm going to do my best not to cover territory that we already covered, but I know we were talking about your report. And did you answer the question as to why it is you did not put your name on the report?

A. I believe I said that this wasn't really a report. It was something that I'd written down to provide for a meeting that we had.

Q. Okay. And is that the same reason why there's no date on it?

A. Yes, sir. I mean, it was done, literally, 10 or 11 o'clock the night before meeting.

Q. Okay. Did you actually refer to your notes while writing the report? Did you ---

A. Completely -- completely from memory.

Q. Okay. If we could, what I would like to do is have you take us through exactly what it is you are alleging Mr. Cooper did on the Google map search that has time stamps that say it occurred on July 11th. And --

THE COURT: Keep your voice up.

MR. KURTZ: Okay.

Q. Now, Officer Chappell, could you say -- and keep in mind I understand the search was 41 seconds. I am not doing this right now to demonstrate how long it takes. I intend to go through this so that we all understand exactly what it is ---

MR. ZELLINGER: Your Honor, I'm going to object. Is this a question?

THE COURT: Let him go ahead and finish. Go ahead.

MR. KURTZ: I'm just trying not to be misleading. I -- I don't want to leave anyone with the impression that this is for the time frame.

BY MR. KURTZ:

Q. If you would just take us through the exact steps that you believe the Defendant performed, when he went to this page. So from -- from this screen ---

A. Uh-huh.

Q. -- what is it that was put into the search box?

A. The zip code 27518.

Q. And, at this point, what was the next action?

A. Well, again, and since we're doing this now three years later, I can't say for sure that the underlying code that this page is run by, is exactly identical to the way it was in July of 2008, and certainly not the way it was in September of 2008 when we did our test because, as you'll notice, the dynamic content under the photos, under the "explore this area," those photos are all different because they're dynamically provisioned at the time that you do your search.

Q. Well, of course that's true, but when was it that you did your test?

A. September of 2008.

Q. And have you ever worked with Google?

A. No, I have not.

A. You were aware that Google updates their code for all of their pages on ---

MR. ZELLINGER: Objection, Your Honor. This is not in evidence.

THE COURT: But he -- he can ask the question and he can answer it, if he's aware. I -- I don't know if it's something of a matter of general knowledge, or what. Go ahead, Mr. Kurtz.

BY MR. KURTZ:

Q. But you testified that it’s not going to operate the same now because it’s changed over time.

A. And it’s very likely that the code to this page, the actual web code, could be substantially different because Google does update its products.

Q. And you don’t know what date Google updates its products?

A. No, sir.

Q. You don’t know what the substance of the -- of those updates are?

A. No, sir.

Q. You don’t know if they update it once every month, or once every hour?

A. I'm -- I’m testifying right now, I have no idea how Google updates their product, when they do it, or how they do it.

Q. So when you did your test, though it was closer in time, you didn’t know then that it would perform in the exact same fashion as it did on July 11th, or on July 16th, whenever the search is performed?

A. No, sir. But my results bore out the same --

MR. ZELLINGER: Your Honor, I --

A. -- results.

MR. ZELLINGER: -- object to July 16th, which is a mischaracterization of the evidence.

THE COURT: That portion is sustained.

MR. KURTZ: But, Your Honor, the question is specifically when this took place. That is the point in contention. It is not that I am adopting July 11th as an accurate date ---

THE COURT: I sustained the objection. You can move on.

BY MR. KURTZ:

Q. You don't know if the code had changed at the time that you actually did your test?

A. No, sir. But I'm satisfied that the results of my test matched the results that I found on the Defendant's hard drive. I'm just -- I'm just stating for the record, before we proceed with any sort of live demonstration, if the underlying code to the Google page has changed, the results may not be the same as the results that I achieved in my test, nor the results on Mr. Cooper's laptop. And I just don't want you to draw some incorrect conclusion, based on the fact that a test done three years later doesn't have the same results. I'm just trying to point that out to you, sir.

Q. Understood, but when you did your test in September, simply because you got the results that you expected, that does not mean the code had not changed prior to that time.

MR. ZELLINGER: Objection to that form of the question.

THE COURT: Overruled.

A. I -- I don't understand your question. I -- I -- I achieved the same results as what was on his laptop, therefore, I don't know if the code was different. Is that your question?

Q. Just because the results ended up being similar, doesn't mean that the code had not been changed in fundamental ways before you did your test.

A. I -- I suppose it could be possible.

Q. So, at this point, what I -- I would simply like to do is go through and have you show us exactly what was done.

A. What I did? Or what I believe the Defendant did?

Q. What you believe the Defendant did.

A. Okay. Then probably what we need to do is go back to the starting page.

Q. Okay.

MR. ZELLINGER: You Honor, I'm going to object to this point. It's clear that there's no foundation for this display. If this was a test that had been run in years prior, then we could have the same results. But at this point, the -- the files that were found on the Defendant's computer, the test that Mr. Chappell had -- compares those to -- to what he did in Google at the time in 2008, I -- I think that this is -- this is more pursuant to Rule 403, this is inappropriate.

THE COURT: In my discretion, I'm going to allow it. It's up to the jury to determine what weight they give this evidence, much as they -- it is their responsibility to determine the weight they give any and all evidence in the case. So, ultimately it's up to the jury to determine what weight they give to all the evidence in the case, including this particular line of questioning. So, in my discretion, I'm going to allow it. Go ahead.

A. In my test, this is consistent with the initial landing page for Google Maps. It's not in satellite view, because I'd never visited the page before on the test computer. The initial temporary internet content on the Defendant's computer was in satellite view. There was a cookie, consistent with previous Google visits, that led me to believe on a previous visit he had set a preference to show the maps in satellite view, so that when he arrived at the landing page it was displayed in satellite view. So if you'll click the satellite view now ---

Q. Okay. Now, before we move on, when you said that there was a cookie that would have dictated satellite view; in fact, you are not referring to a cookie from the July 11th visit, are you?

A. No, sir, I'm not.

Q. Okay. Just to be clear, there was no cookie from a July 11th visit to Google Maps?

A. No, sir. And I wouldn't expect there would be.

Q. Okay. I'll -- we'll talk about that in a bit. But for right now, could you please explain the next step that was taken.

A. Could -- could you navigate to some other page, maybe your -- your home page or just to move away from the Google page for a moment --

Q. Okay.

A. -- and then back to the maps page now? So the initial landing page, as you can see, because we've previously visited the page, put it in satellite view. When we go back to the page now, it's in satellite view for us. That would be consistent with the initial temporary internet content.

Q. Okay.

A. If you would now type in 27518.

Q. Okay. And what's the next step?

A. At -- at this point, in order to get tiles to the level of magnification of Fielding Drive, you would need to zoom the map in, and scroll the map over.

Q. And how is it that you believe the map was scrolled and zoomed? Quite specifically, what exact actions to you believe were taken?

MR. ZELLINGER: Your Honor, I'd just like to put something on the record at this point that before we got to this part the web browser was widened by whoever was operating it. And I think that's important for the record purposes.

MR. KURTZ: That the web browser was what?

MR. ZELLINGER: The -- the window was made bigger 20 seconds ago. The -- the window was made bigger on the left side. I think that needs to be reflected in the record.

THE COURT: All Right.

MR. ZELLINGER: Okay.

Q. What--what --

THE COURT: So -- so my -- I -- what -- what the jury is seeing now, is this what the State contends--

MR. ZELLINGER: No.

MR. KURTZ: I'm about to --

MR. ZELLINGER: No. Because what just happened already took it out of what Investigator Chappell just did. So ---

MR. KURTZ: I'd just asked what it is that -- what you prefer, and I'll adjust it.

MR. ZELLINGER: I -- I would prefer that this be done in 2008 in the -- the same laboratory manner that

Investigator Chappell did it. I don't have a problem if we keep doing this. I understand it goes to the weight, but I think that the record needs to reflect that the window was made bigger. The left side was extended out. This isn't a full page view of -- of Google Maps. It was manipulated so the Window got bigger. And I just want -- think that the record needs to reflect exactly every action that's done on this computer at this point.

MR. KURTZ: And so -- I'm just curious as to how you would like the window. We'll format it that way. I can't go back to 2008.

THE COURT: The objection's noted for the record. You may proceed, Mr. Kurtz. Once again, all this goes to the weight, and you can ask whatever questions on redirect if you wish.

MR. ZELLINGER: Okay.

A. I think your question to me was, specifically, how was the map scrolled, how was the map zoomed?

BY MR. KURTZ:

Q. Right, And that -- the reason I asked that question is, there are several different levels of zoom that exist in the temporary internet files, correct?

A. Yes, sir.

Q. And that means that at each time, the entire page populated with tiles.

A. Additional tiles are loaded every time the map is manipulated in some way to reflect whatever area the person has selected.

Q. And every block on the screen, as well as the -- the adjacent blocks that are off of the screen, populate in the -- the images loaded onto the hard drive at that time; is that correct?

A. When you say the blocks that are off the screen, I’m not sure I’m clear on what exactly it is you're saying.

Q. Well, Google -- are you aware that Google actually buffers information for surrounding tiles so that when someone navigates, that it navigates faster?

A. I would -- I would just want you to clarify. When you say buffer the tiles, how big of an area is -- is it that you believe they buffered.

Q. I’m not specifying an area. I’m -- I’m simply saying that there are tiles that would not be reflected on the screen that are already loaded into the temporary internet files.

A. I would say that’s somewhat inconsistent with my findings, and the findings that were on the Defendant’s computer. That may be a functionality of the way it works now, but if -- if you’re saying that just by going to this map, there’s going to be tiles for the Outer Banks of North Carolina, of Washington, DC, just by going to this view at

27518, I would say that's inconsistent with the testing.

Q. That's not what I said.

A. Well, that's why -- that's why I asked you to clarify how big of an area.

Q. If we were talking about a single tile in each direction, would that be consistent with your understanding of how it works?

A. That -- that would be more accurate, I would say.

Q. Okay. Then, for the purposes of discussion, let's talk about it in those terms. That's fine. So the reason we were talking about this is, when I asked for you to tell us exactly what's done, I want to know when you were saying -- is it a click, a hold with a closed hand and a drag of the screen, or is it a drill down by double clicking on a spot, to tell us exactly what it is that you believe Mr. Cooper did and exactly how he did it?

A. I believe this screen was clicked upon and had to have been manipulated, because that was the only way I was able to get a closed hand cursor file to appear in our temporary internet folder in our test machine.

Q. Okay.

A. That -- that did not appear by us just going to the page and doing nothing.

Q. I -- I understood your testimony. Just tell us where you want us to click and how to click and we'll do that.

A. Well, in order to go to Fielding Drive, you would need to click on the map and drag the map so that the map moves to the left.

Q. And we'll click on it and start dragging left. You tell us when to stop.

A. So, right now the -- as you're clicking on this, are you double clicking the map? Because it's magnifying.

Q. Yes we are. We ---

A. Okay. So that's one way to do it. The other way that it could be done, is the map could be clicked upon and dragged over and then the -- the scroll, the map control, that could be moved. If you have a wheel mouse, you could move the -- the wheel mouse. Are you -- are you asking me to divine somehow, from forensic artifact, the specific sequence of which particular method was used to zoom the map -- or move the map? Because I can't do that.

Q. Well, you -- you can to some extent, can't you? In fact, you testified that you could to some extent.

A. I testified that the map had to have been moved, and I testified that the map had to have been zoomed in.

Q. Well ---

A. Are you asking me to -- to specifically say how I believe the mouse was used?

Q. You were talking about the open hand versus the closed hand. And that only occurs when you click and drag on the screen; is that accurate?

A. When you interact with the map. So clicking and dragging would be interacting with the map.

Q. But going to the zoom level would not actually give you an open and closed hand at that point? It would give you an arrow cursor, wouldn't it?

A. You're saying just clicking to -- double click to zoom the map down -- or it's not dragging the map, not manipulating the map, zooming in?

Q. Yes.

A. I -- I think that's consistent with what I said. I said you have to click on the map and drag the map. You have to manipulate the map. Just zooming in is not what I testified to, sir.

Q. And how many different levels of zoom were actually used?

A. I -- I believe I testified that the default level is 11 based on our testing and that the -- the level of zoom was very close to almost the maximum level, based on the artifact on our test machine, comparing that to the Defendant's machine.

Q. That's not exactly the question I'm asking. I'm asking, how many separate levels of magnification did you find for tiles?

A. I -- I don't think I understand what you're asking me. I mean, I ---

Q. Okay.

A. -- I don't know that I can correlate a specific tile to a particular magnification level because the artifact does not reflect that.

Q. That would be maximum zoom right there, correct?

A. Yes, sir.

Q. And that was done with a single click, correct?

A. I don't know how it was done. I didn't do it.

Q. You can determine by looking at it. What other mechanism do you believe was used to just do that?

A. To zoom in? As I've testified, you can either double click on the map, you can use a scroll mouse, you can move the magnification level.

Q. But we just went five levels of zoom all at one time; is that right?

A. I don't know, sir.

Q. Okay. Let's go to maximum, or the least magnification, the entire planet. Now, if you go to the highest level of zoom. So, doing it like that ---

A. Moving the magnification level bar, yes.

Q. That -- that actually changed the magnification by what, eleven levels all at once?

A. I -- I'll take your word for it. I -- not counting the bar.

Q. More than six? Well, you can take a look and--

A. Certainly the magnification was increased, yes, sir.

Q. What -- how many levels -- is it as least six levels that that magnification moved?

A. I mean, would you like to -- to count each step?

Q. Go ahead, tell us how many.

A. I -- I can't manipulate the map from here. I mean ---

Q. Can- -- -go -- go to the bar and just move -- move the -- the bar down. It appears to be 20 levels.

Q. Okay. The way that we just did it, on some of the steps, you were able to see it populate the screen. You saw all the titles on the screen.

A. Well, it has to load the tiles to the level of magnification being viewed, so yes, sir.

Q. On other levels it did not, because we moved so quickly that it never had time to do that.

A. That's an accurate statement.

Q. The question that I'm asking, with respect to Mr. Cooper's computer is, how many separate levels of magnification did you find where there were completely populated screens?

A. I -- I don't believe I can answer what you're asking because I can't look at the artifact in the way the web browser sees it. I think when we showed the -- the folder with all the individual tiles in it, the only way I have to know when those tiles were created, is the time stamps on the files. The order and sequence that they appeared on the hard drive. And that would be consistent with navigating to a particular page.

Q. You stitched together those tiles, though. That was your testimony.

A. Yes, I did, because these were all tiles that were created on the hard drive contemporaneously. They all matched in area on the test computer, so, it's -- it's quite easy once you know, here's, you know, nine tiles. They were all created sequentially. They appear to be tiles that represent this street.

Q. And you actually talked about following through the mechanism by which you were able to reassemble all of the different screens that you had.

A. I -- I don't believe I testified that I assembled every single tile, because I did not.

Q. Did you realize when you were looking at the tiles, that some of the tiles were obviously shot from further away and some of them were shot closer?

A. Clearly, because some of the initial content is at a much greater zoom level. It's not as magnified as some of the later content.

Q. How many different levels did you focus on during your examination?

A. There was the initial content that showed Fielding Drive. And then, there was much more magnified versions of Fielding Drive, up to and including the area where Nancy Cooper's body was found.

Q. Is there -- you time lined out exactly how much time was spent at each place, did you not?

A. Well, I knew how much time elapsed between the first temporary internet artifact and the last temporary internet artifact associated with Google Maps.

Q. And it's significant -- it was significant to you enough to testify that -- yesterday -- that there was three seconds spent at the highest level of magnification on Fielding Drive.

A. I don't think that would be an accurate reflection of my testimony. Those tiles were all created in that span of time. I never testified as to how long anyone would have stayed on the page. I have no way to know that.

Q. You're unaware as to whether or not -- whether the browser was closed after that?

A. I'm not sure I would be able to know how the browser was operating, based on the temporary internet content at Google. I know there was temporary internet content. I know when it stopped. Whether or not the browser remained open after that time, I'm not in a position to say, looking forensically at temporary internet files.

Q. When you say you're not necessarily in a position to look at something based on temporary internet files, you are in a position to determine how many complete screen shots were allowed to refresh, aren't you?

A. I -- I don't think I understand what you're asking.

Q. At every level of zoom, it requires its own separate set of tiles?

A. If -- if your question is, did I reassemble every single page between the time that the Google Maps page was navigated to, to the time that the Google Maps artifacts ceased, no I did not.

Q. The first question was actually, you were capable of doing that?

A. I don't know that that would be an accurate statement. There, as I testified on direct, there were a number of portable network graphics files -- the clear overlay files -- that because there were no streets or any sort of artifact to give me an idea where this particular clear overlay was, I can't say with any specificity that a particular tile that's a bunch of trees, goes in this particular area.

Q. Isn't there code that exists well beyond just the picture that you're looking at?

A. When you say code, can you be more specific? Are you asking about hypertext markup language, or you asking about Java Script, or are you--

Q. I'm asking about- -- -asking about- -- -hypertext.

A. This Google Maps artifact, aside from the landing page, that's maps at HTM, it's not created as a traditional hypertext markup page. There's a framework that is the hypertext markup, and then there's Java script. And because most of this content is dynamically provisioned, it requires these calls to be made to the Google servers and the Google servers serve up that content dynamically. That's one reason that we can't recreate these pages the same way that we can recreate, like a Google search, or some of the traditional HTML web pages. Because all that map area is dynamically provisioned.

Q. Every single time that a hand clicks and drags, it creates an artifact on the machine ---

A. It --

Q. -- correct?

A. -- creates an artifact, but it does not create, you know, a specific record that explains how to assemble that artifact. That's what Google is doing in the background to render that page.

Q. But every time that you were able to determine if something was clicked and dragged, you could then look to see how long afterward there was a next occurrence of a hand dragging?

A. No, sir. That's not accurate.

Q. Why is that not accurate?

A. Because the closed hand cursor fall only is generated once in the temporary internet content. It's a Java Script call. It changes the cursor from an open hand to a closed hand. You don't get a closed hand cursor every time you click on the map.

Q. And so you have no idea how it is that the screen goes from the initial landing page of 27518, to the Fielding Drive location?

A. I know the only way I was able to replicate it was by dragging the map over and zooming in, sequentially, until I zoomed to a level in which the test artifact was substantially similar in appearance to the artifact on the Defendant's computer. No, I do not know exactly what steps were taken. I was not there.

Q. Did you attempt to figure it out?

A. I -- I believe I did.

Q. Is there a reason that somebody who is not trained as a forensic examiner would be able to stitch together all of the pages without a problem, but you're unable to?

A. Again, if -- if the code is changed substantially in three years, and the tiles are rendered in a different way, or there’s additional artifact that gives you some indication as how these were put together, I -- I can't -- I can’t explain that. I can’t testify to something that I didn’t do.

Q. I -- I’m not talking about in 2011. I’m saying with the artifacts on Mr. Cooper’s computer. Does that -- is your testimony that you do not believe that we would have been able to stitch together each separate page from that internet history?

A. No, sir. My testimony is that I did not.

Q. Why is it that you didn’t do that?

A. I created the artifact on the test computer that replicated artifact on the Defendant’s computer. I didn’t have a way to do every single page, every single view, every single magnification change. I -- I performed to the best of my ability.

Q. Did you believe that it might be significant as to how it was that that material ended up on the computer?

A. I don’t understand. How -- how do you mean? I don’t understand how it’s significant?

Q. Is it your theory that Mr. Cooper was, on July 11th, searching around for a place to put his wife’s body?

A. That would be consistent with someone going to Google Maps, typing a zip code, moving the map to the area where the body was found, and zooming into that location.

Q. Now, if somebody went directly to that spot and zoomed into the highest level of magnification in a 41-second span, that would indicate that someone already knew exactly where they were going, wouldn't it?

A. I -- I was able to move that map in a lot less than 41 seconds when I did it after the fact. So I -- I guess, you know, 41 seconds is a long time if you actually sit for 41 seconds.

Q. But isn't part of that why the question of how many separate levels of magnification fully populated could be important?

A. I mean, whether the person zoomed immediately or whether they zoomed incrementally, the -- the fact remains for me, that the content was on the computer, the content was at a very great level of magnification, beyond the starting level of magnification, just by going to the search term 27518.

Q. The question is, if someone -- as somebody zooms in, level by level, if they're allowing a page to populate fully, that takes additional time at each step?

A. I think that would be subjective, based on the internet connection speed that the person has. Someone who's on, you know, a DSL modem that might not have as much bandwidth as someone behind a corporate network with a much larger, faster connection to the internet, the speeds would be different.

Q. Is there any -- any way physically possible that somebody could go to multiple levels at the exact same moment in time, allowing the screen to populate completely each time, in as short a period of time as just clicking five levels ahead?

A. I -- I suppose anything is possible.

Q. Have you ever, as a forensic examiner, encountered a situation where somebody could do anything like that?

A. I've never encountered a situation before involving someone clicking on a map.

Q. When you -- when you looked at the map, did you note the path that was taken to go from the 27518 zip code over to Fielding Drive?

MR. ZELLINGER: Objection, Your Honor. This has been asked three times.

THE COURT: Sustained.

BY MR. KURTZ:

Q. Well, could you show us exactly what it is you're saying was done?

MR. ZELLINGER: Same objection.

MR. KURTZ: We never got past the first page, Judge.

THE COURT: Overruled. Go ahead.

A. If you would just move the map over slightly, so that Fielding Drive can be seen. Zoom in and zoom in. You're going to have to move the map so that Fielding Drive can be seen. I mean, as you can see the cul-de-sac, it needs to be zoomed in. Obviously, it needs to be zoomed in.

Q. Okay. Keep directing us as necessary.

A. I would say the map also needs to be moved a little bit more, zoomed in some more. Zoomed in some more. I think the map needs to be moved, a little bit down slightly. Obviously that's aerial footage from a much more recent time, but I think that's similar to the content that was seen on the Defendant's computer.

Q. Okay. And so a number of intermediate steps are required to actually get to that point?

A. As I testified, the map has to be moved. The magnification has to be increased.

Q. Did you see any evidence that there was searching around in other areas of -- of Cary?

A. During that 41-second span of time? No, sir.

Q. So your testimony is that you believe Mr. Cooper went directly to that spot.

A. I -- I don't know how long it took him to get from the starting point to the ending point, and by what path he -- he went to that. I know there's a lot of artifact for Fielding Drive. And there's much greater levels of magnification to this part of Fielding Drive, where Nancy

Cooper's body was found.

Q. And for every tile that you were hitting, there are actually two sets of graphics that have to load; is that correct?

A. As I testified on direct, yes, sir.

Q. Now, you're familiar with Special Agent Johnson's report on the computer?

A. Somewhat, yes, sir. I don't have the report right in front of me.

Q. You are aware that on other computers, Special Agent Johnson referred to checking for cookie files?

A. I -- I'll take your word for it. I don't have the report right in front of me.

Q. Do you know that Special Agent Johnson doesn't mention anything about cookies in his report on Mr. Cooper's computer?

A. I do not know one way or the other.

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

THE COURT: You may.

Q. I'm showing you what's been marked as Defendant's Exhibit 83. It's actually in evidence already under a different number, but that is Special Agent Johnson's report, correct?

A. I will assume so.

Q. Well, if you simply look through, does it say at the bottom who wrote the report, on the very first page?

A. It does. I'm looking to see how many pages are present -- the last page is actually pertinent.

Q. I promise I won't ask you to read from the last page. If I could hold this for a moment and direct you specifically to the section on QCE31. The summary of examination results. If you could please read it through to yourself, and afterwards I'll have a question for you.

A. (Witness complies.) Okay.

Q. At any point in Special Agent Johnson's report, does he note any examination for cookies on that computer?

A. Not on Page 13. No, sir.

Q. You can check the next page if it still pertains to QCE31. In fact, I believe that's everything on QCE31; is it not?

A. Nothing is mentioned on this page. No, sir.

Q. Is there -- well, if you're limiting it that page, is there anything in that report that says anything about cookies on QCE31?

A. There's nothing on this page that refers to summary of examination results for QCE31.

Q. And is that, in fact, the only summary of results on QCE31 in that report?

A. I -- I don't know without ---

Q. Take ---

A. -- looking at every single page.

Q. -- take a look.

A. I didn't prepare this report. (Witness reviews document.) No, sir. There's no specific mention of cookies.

Q. Thank you. Now, by contrast, in the summary of examination results of QCE21, does it talk about actually performing an examination for cookies?

A. Yes, sir.

Q. Thank you. What is the significance -- actually, you -- you were here yesterday for Special Agent Johnson's testimony. Did -- did you agree with what he testified to with respect to the significance of cookies?

A. Cookies are website preferences. They're normally set when one visits a website.

Q. And you heard his testimony about how a cookie has a unique identifying characteristic that would allow you to do a court order to the provider?

A. Yes, sir.

Q. And the information that you could get from the provider, if you provided them with that unique identifier, would allow that provider to give you information that they have on their servers about the visit to that website?

A. That's accurate.

Q. That is, in fact, a way of getting the server, like Google's servers, time stamped for when an action occurred?

A. That's accurate.

Q. It is essentially a bulletproof way of verifying when something happened?

A. Well, again, that's -- that's sort of subjective because I'm sure if, you know, there was a server stamp, someone could always make the argument that the server stamp was somehow invalid.

Q. If the server stamp was invalid, as well as the local machine -- so somebody hacked into Google servers, changed that time and changed the local time on a machine?

A. I'm -- I'm just saying it's -- it -- it's sort of subjective to say it's a bulletproof ---

Q. Okay. You said that you believe there was a cookie for this visit?

A. I know there was a Google cookie that was set. And I believe there's actually, I think, nine different Google cookies, if you count a specific cookie relating to Google advertising ones.

Q. And you actually -- you're familiar with the report that was prepared by Mr. Ward on tampering on the Think Pad?

A. Yes, sir.

Q. And you've gone through that report?

A. Yes, sir.

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

THE COURT: You may.

Q. In the appendix -- well actually I'm showing you what's been marked as Defendant's Exhibit 84. Do you recognize this as being Mr. Ward's report on tampering on the computer?

A. It appears to be.

Q. Okay. If I could refer you specifically to Appendix D and E. If you could look over Appendices D and E and tell me if -- in fact, those entries contain both the active and the deleted cookie files that were on Mr. Cooper's machine, including Google.

A. (Witness complies.) I believe there might be one missing. Yeah, there's one missing related to Google Ads.

Q. Related to Google Ads?

A. Right.

Q. Google Maps and Google Ads are different animals: are they not?

A. Yes. Google has a number of products.

Q. And Google Maps actually does insert its own cookie into a machine when somebody visits?

A. I would say that's incorrect.

Q. What would you say is the case?

A. Based on the internet artifact that was present on the Defendant's machine and testing that we conducted, Google sets a cookie and that that one Google cookie can be used for multiple services. That's why from a Google landing page, on a search term, for example, you can set preferences for a search, click on the maps page, set preferences for the maps -- like the satellite view -- click on your Gmail account, have preferences in that. And one cookie can control all those functions because the cookie's a unique identifier for your specific machine. Google's controlling the information. They recognize your machine's visiting their site, their service. And if you've configured certain preferences, then those preferences can be displayed from that one Google cookie.

Q. You are aware that different types of Google, or different applications that Google runs, actually have their own separate flavor of cookie; are you not?

A. No, sir. I don't think that's accurate.

Q. You're aware that on Mr. Cooper's computer, there were Google cookies one, two, three, five, six, seven, and eight; are you not?

A. Yes, sir. But they were for different things.

Q. And Google cookie four was nowhere on the machine, either in deleted or inactive files?

A. No, sir.

Q. You say that it's possible that one of the other Google cookies had been updated at the time of the July 11th visit. Are you able to show us that cookie?

A. I -- I don't have any way of knowing. I suspect it was a cookie related to Google.com, because the other cookies that I found were related to a Google site, Google.ie which would be Ireland; Google.it, which -- which was deemed to be Italy; Google.com/verify, which seems to be associated with some sort of validation or verification scheme; Google.com/international; Google.com/accounts; Google.com/mail/help.

Q. You're aware that there is a considerable amount of information that's contained inside a cookie; are you not?

A. By "considerable," I don't know that I would -- I would say pages and pages of information. There can be some time stamps that are contained. There can be unique identifier that is something that, you know, a site provider uses. But --

Q. Okay.

A. -- I wouldn't say considerable.

Q. How about significant data? Would you say that the data inside a Google cookie can be significant? Particularly significant in a criminal investigation?

A. There's data about the first time, potentially, someone visits a site, the last time they visited a site, if any preferences were modified, if they were referred from another URL to that site. So, I -- I think it's fair to say that, yes, there can be important information in the cookie, but I would just not be comfortable saying, like a significant volume of information.

Q. So is it your testimony that intermediate access to Google would not be reflected in the cookie? So if you went to Google four times, and you're only going to see the first create date and the last visit, but you're not going to see the two visits in between?

A. You're saying if -- if you only get one cookie that it's set?

Q. If you're only dealing with one.

A. There's a number of times -- it tells you how many hits for that particular cookie.

Q. And ---

A. Like for the Google.com cookie, there were 92 hits associated with that cookie.

Q. And within the Google cookies, are you able to isolate any one that was created -- there are no cookies that's -- there are no -- not a single Google cookie on that computer that spans July 11th, is there?

A. Not specifically, no, sir.

Q. So they're created prior, and the last modified is prior to July 11th. That's one set of Google cookies; is that accurate?

A. Yes, sir.

Q. Then there is a set of Google cookies that is created on the 12th or later and modified on the 12th or later. Is that a correct statement?

A. I think so.

Q. There is not a single cookie that exists or existed in a fashion that it was modified on July 11th?

A. You mean existed and was deleted at some point?

Q. Well, deleted cookies appear here, don't they?

A. If they're recoverable, they would appear. If a file has been deleted and is overwritten, it cannot be recovered.

Q. Is your testimony that there is a Google cookie on the machine that matches up with this -- with this search? Or is your testimony that the cookie must have existed, but is has since been irretrievably deleted?

A. What you asked is, if there was a cookie that ever existed? And I -- I can't say that, because if it was deleted and overwritten, that would not be recoverable.

Q. That's not the question I'm asking. The question I'm asking is, is there a cookie that exists on the machine that you looked at, that existed on July 11th and was either modified on July 11th or has a modification date that would have included July 11th?

A. Nothing in allocated or recovered deleted, no, sir.

Q. And so the answer is, there's not a single cookie on the machine that corresponds to that visit?

A. Not that we can see from this side, no, sir.

Q. Do you recall writing something that may or may not be a report that we have discussed?

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

THE COURT: You may.

Q. Are you able to -- this is your report, correct? This is -- has previously been marked as Defendant's Exhibit 77. And in it, do you not say that there is a cookie that corroborates this particular visit on July 11th?

A. At that time, I believe there was.

Q. So that statement in your report was untrue?

A. I would say the statement is inaccurate. If you read the entirety of that statement, it goes on to specify some information from a Google server that could corroborate this visit. It was my belief at the time that that was written, that some information had been obtained from either a search warrant or a court order.

Q. That's a great question. You can use a search warrant or a court order to get information from Google that would corroborate any particular activity, correct?

A. You can, potentially.

Q. You worked with Special Agent Johnson on this case.

A. I did.

Q. He is an extremely experienced computer forensics examiner?

A. Yes, sir.

Q. At no point did either of you, working in tandem, identify a cookie that went along with this particular search?

A. Again, as previously stated, I couldn't find a cookie specific to this Google map visit.

Q. Had you found a cookie, that would have been an extremely significant item of evidence, wouldn't it?

A. We found a number of cookies.

Q. Had you found that particular cookie, that would have been an extremely significant piece of evidence?

A. It would've been nice to have, yes, sir.

Q. And once you would have that cookie, you would take it and subpoena or court order Google to provide their server logs?

A. You could do that for any cookie that's a Google cookie. It doesn't necessarily have to be specific to that visit. As I previously testified, if there's a unique identifier for a cookie, it relates to a specific machine, So any cookie could be given to Google and they could see what that cookie related to.

Q. At no time did anybody seek a court order from Google for that information?

A. Is -- is that what you're telling me? I -- I never sought anything. Information was provided to the investigators of the case. But I never personally sought anything and I can't speak for the actions of anyone else.

Q. Well, as an investigator, as a forensic investigator in this case, it is your job not only to investigate the information on the computer, but also to advise law enforcement as to recommended course of action; is it not?

A. And I did.

Q. And did you explain to law enforcement that the appropriate course of action would be to send a court order to Google to find out the details of that particular user I.D.?

A. I believe we sent a preservation letter on behalf of the Cary Police to preserve that data.

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

THE COURT: You may.

Q. I'm showing you what's been previously identified by Special Agent Johnson as a preservation letter that was sent to Google. The information that is requested to be preserved does not include user information related to any cookies on that computer, does it?

A. Preserve for a period of ninety days, any and all records and other evidence including, but not limited to, groups, search history, talk, Google checkout, logs, log files, emails sent to and from the following Google account user for the listed dates and time, account BB simple at gmail dot com, account creation date to present. It's also requested that any and all records of the user information of the individual, who was or were assigned this email account for the time frame, be maintained. This includes, but not limited to, subscriber identity, billing information, mailing address, credit card information, et cetera. If it's determined that the individual using this email connected from another IP address, it is requested that this IP address also be preserved.

Q. Now, that is specific to the email address BB simple, correct?

A. And any associated files with that email address.

Q. And there is no user I.D. from a cookie specified?

A. There wouldn't be a user I.D. It would be a unique identifier. But, no sir.

Q. There's no unique identifier in there. There is similarly no identification requesting that any information pertaining to a search performed at approximately 1:15 on July 11th be preserved?

A. No, sir, not in that preservation letter.

Q. And that, too, would have been a way to ensure that the data was maintained at Google?

A. Certainly.

Q. You were aware -- well, actually, you heard Special Agent Johnson's testimony yesterday, but you're also personally aware that Google, in 2008, had a privacy policy, correct?

A. Yes, sir.

Q. And that privacy policy was nine months?

A. It was nine months for IP addresses. After nine months, the IP addresses would be anonymized. It was 18 months for cookie information.

Q. But when you say anonymized, that would anonymize the cookie information, as well, would it not?

A. After- -- -not.

A. -- eighteen months, presumably.

Q. If that were true, you believe you would have had 18 months to actually seek confirmation from Google about the time that their server was hit with a search that ends up at Fielding Drive?

A. Eighteen months for them to go back and corroborate a particular cookie that they're provided. That's what their privacy policy states.

Q. So, when you say that you weren't able to find a cookie for that visit in either deleted or undeleted, does that mean -- what does that mean to you?

A. Just that. It wasn't a recoverable deleted file and it wasn't in allocated space, still on the temporary internet content somewhere.

Q. And that would -- you did find plenty of other

Google cookies though?

A. Yes, sir.

Q. That predated and postdated?

A. Yes, sir.

Q. And a great deal of other cookies from other providers?

A. That's correct.

Q. So is it your opinion that Mr. Cooper intentionally deleted a single cookie off of his machine? And then, I assume the term would be shredded that file, so that it would be completely unrecoverable?

A. I suppose that's a possibility.

Q. And you're aware that Mr. Cooper has a degree in Computer Science?

A. Yes, sir.

Q. You were, when you were doing this examination?

A. No, not at the time.

Q. All right.

A. I knew he was employed at Cisco in some sort of voice-over IP capacity.

Q. It does not strike you as inconsistent that someone would go to the trouble of finding an individual cookie and deleting it, but not delete temporary internet files that are associated?

A. I can't speak to why people do certain things.

Q. But you're aware that Internet Explorer had, at that time, private browsing mode?

A. Yes, sir.

Q. And that Internet Explorer had a one button clean up all of your temporary internet history, as well as your cookie files, capability?

A. The browser was Version 7. I think that's consistent.

Q. All right. So to actually purge all that information would take seconds?

A. I suppose.

Q. You also spoke about -- or actually, I think it was Special Agent Johnson who spoke about Mr. Cooper, on the morning of July 12th, navigating to a number of web sites?

A. Are you asking if I'm aware of ---

Q. Are --

A. -- that?

Q. Are you aware that Mr. Cooper, in his internet history, shows that he went to the Museum of Life and Science?

A. Yes, sir.

Q. Natural History Museum? Looked up the cost of power washing a house?

A. Yes, sir. I think all that was testified on direct.

Q. Did a number of -- of different searches?

A. Yes, sir.

Q. Is that -- is that consistent, in your mind, with somebody who had killed their wife the night before?

A. Well, I suppose it -- it could be a thing you would do if you're trying to establish an alibi that -- I suppose that's possible.

Q. A digital alibi, essentially?

A. Sure.

Q. You don't find it inconsistent that a man who is attempting -- a man who is aware of that internet activity in the morning, leaves temporary internet files that somebody can find -- somebody can say, this is what he was doing at this time? You don't find inconsistent that that same person would supposedly leave a 41-second search of the precise spot where his wife's body was found?

A. Sir, in my career as a law enforcement officer, I've had people do the -- the strangest things. I've -- in a span of -- of a month's time, I think I processed three different cell phones from people who committed violent assaults against other people and, in the course of fleeing from those assaults, dropped their cell phone at the scene. I had a person who handed a -- a bank robbery note to a teller and left his drivers licence on the counter. I had someone who committed a series of frauds using a -- I guess what he assumed was an anonymous Yahoo email account that he had linked to a social networking profile for himself. I -- I can't explain why people do certain things.

Q. In -- your career as a law enforcement officer includes being an airport policeman?

A. For two years.

Q. And you were actually the lead investigator, for a while, in Duke Lacrosse, weren't you?

A. No, sir. I had no involvement in the Duke Lacrosse.

Q. You didn't respond in that case?

A. No, sir. I was out of town at a training conference at the time that that case happened.

Q. You talked about social networking as being a subject of relevance in one of your prior investigations?

A. Yes, sir.

Q. Has that come up since that time?

A. That specific case or -- we use social networking sites all the time to locate criminals, fugitives, find missing -- missing children.

Q. And you evaluated Ms. Cooper's Apple laptop?

A. Yes, sir.

Q. You did not note that Ms. Cooper was a user of Facebook.

A. Specifically in my report, no, sir.

Q. And you did not note that she had only actually used Facebook one time on that computer?

A. I don't remember noting anything in specific about Facebook.

Q. But you did notice her Facebook activity when you did your examination?

A. I believe I noticed a -- a couple of Facebook cookies. It wouldn't -- it wouldn't be a significant amount of Facebook activity at all, compared to other cases that I've evaluated.

Q. But you're aware that people can use Facebook on Smart phones?

A. In July of 2008, I'm not sure what functionality would have been available for Facebook Mobile.

Q. Did you look into it?

A. I don't believe there was a significant amount of functionality for Facebook Mobile in July of 2008.

Q. Did you look into it?

A. In -- in that -- my experience with Facebook from previous investigations, I don't believe that's a significant way of utilizing Facebook through mobile interface at that time frame.

Q. Going back to Mr. Cooper's computer, did you -- you showed us with net analysis how you were able to actually reassemble web pages.

A. Well, I would classify that as net analysis, reassembling the web pages, I mean.

Q. But net analysis has that functionality?

A. It does, assuming all the internet artifact is present.

Q. But net analysis was not capable of rebuilding the Google map search, was it?

A. No, sir. And I wouldn't expect it, because as I testified, a lot of that content is dynamically provisioned through Java Script.

Q. Did you ever evaluate any routers in this case?

A. No, sir.

Q. Did you evaluate any of the other hardware in this case?

A. By "hardware," what do you mean?

Q. I mean, were you involved in the search of other computers? Were you involved in any search in relation to the modem? What did you do aside from the Macintosh and the IBM?

A. I think, as I've testified, there was an external drive that was formatted HFS Plus File system. It was associated with the Mac Book.

Q. And is that the only other forensic work that you performed in this case?

A. Aside from, I think, maybe looking at thumb drive that had some artifact indicating that it was used in connection with ---

MR. KURTZ: Objection ---

MR. ZELLINGER: To his own question?

MR. KURTZ: I'm going to allow him to finish the answer. I'm ---

A. A -- a thumb drive in connection with Vista artifact related to Ready Boost.

Q. And, speaking of thumb drives, you're -- you are aware that there are programs that will run off of thumb drives and not leave any traces whatsoever on the computer itself?

A. Traces of the file that's being run, or traces that a thumb drive was associated with the computer?

Q. Either.

A. If you associate a thumb drive with a computer, an entry is made in the ENUM portion of the USB store in the registry. So, I would say that's inaccurate.

Q. And you'd have to erase the registry entry?

A. You would have to do something to modify that registry entry.

Q. But it -- it is modifiable?

A. I -- I don't know that you could do it from the thumb drive that you've inserted.

Q. You're aware of -- you're familiar with the program Interpreter?

A. Home Interpreter is a component, I believe, and that is web framework.

Q. You're familiar with MESBOY Framework?

A. Somewhat, yes, sir.

Q. Social Engineers Toolkit?

A. The Social Engineer Toolkit, SCT, yes, sir.

Q. Defiler's Toolkit?

A. I've -- I've heard of that one.

Q. All free, out of the box, essentially, hacking solutions?

A. I -- yes, sir. But are you asking if any of those were -- could have been used in this particular case?

Q. What I asked was, if you're aware of those packages?

A. There's -- there's a number of hacker tools available, yes, sir.

Q. And they're available for free download, correct?

A. Yes, sir.

Q. In your report, you talk about people noticing -- potentially noticing a car right outside the Cooper home. Somebody was going in through wireless. You're aware that the -- the router in the Cooper home was a CISCO 971 -- 871, I'm sorry?

A. Yeah. I think -- think that's correct, the 871.

Q. Commercial grade in terms of signal strength.

A. Yes, it's quite nice.

Q. And 100 and -- over a 100 yards of projected signal?

A. Well, I think that's somewhat subjective because, when they do that testing, they do that in unobstructed areas, so -- I mean, the other thing about a radio frequency is an antenna doesn't necessarily emit things in a perfect circle. And if the wireless router is in a particular place in the house where its signal is blocked in certain directions, I don't think it would be fair to say a 1000 yards in all directions.

Q. You're aware that the specification, however, is that that's the range of the router. And I believe I said a -- 100 yards.

A. If that's the specification, it's under ideal circumstances. I believe the specification also has a -- an inline intrusion prevention system that's an integrated part of that particular router, as well.

Q. With -- you talk about protection systems, you're aware that the protection in the Cooper home was WEP encryption?

A. The wireless security key for the home wireless network?

Q. Yes.

A. Yes, sir.

Q. And you are aware that that is the lowest possible type of encryption that somebody can be running?

A. Yes, sir.

Q. And that it is readily crackable?

A. Well, in that, if you are close enough to obtain signal from the access point, and you have enough time to gather enough packets to reassemble the network key, and have enough time to crack those -- that key for the password, then you can get the password. And then you still have to connect to the network.

Q. But you're aware that -- that actually penetrating WEP can take place in mere minutes?

A. With -- with a good computer and a good processor, this also assumes if the -- the password for the network is -- is not a robust word. Certainly it's very quick to crack it, if it's a dictionary word.

Q. And you're also aware that the computer was left on for 27 hours after it was outside Mr. Cooper's control?

A. I know it was left on. I'm not sure exactly how long but, I think that's -- that sounds about right.

Q. You're aware that is was left on a wireless network for that entire period of time.

A. I know it was, based on some of the artifact that we found on the computer.

Q. There were approximately 692 files that shows modified during that period of time?

A. That -- that sounds about right.

Q. Did you go through and eliminate each file to determine exactly what it was?

A. With Agent Johnson, yes, sir.

Q. And did you actually compare the hash signatures of those files, or did you simply look at them and determine -- well, this looks like an update? How did you do that?

A. We looked at where the files were located. And it's my recollection, none of those 692 files were located under a user profile that would indicate, like a Microsoft Word document being created, an internet page being visited, anything like that. The files that I remember seeing were all in paths consistent with Alterus, which is a software product that Cisco has, that manages the Windows updates and the security updates.

Q. You did note that there were four index dot dat files, which are files associated with Internet Explorer, that were all modified on July 16th, correct?

A. They're internet histories, yes, sir. And they appeared that the reason that they were modified was because of an MS feed application. It's something integrated into Vista that goes out and checks for RSS feeds to see if any of the feeds have been updated. And if they have, then I would expect, because that's a normal behavior, to update that index.dat file.

Q. How is it that -- they're always exactly four index.dat files; is that right?

A. I don't think that would be an accurate statement.

Q. How many index.dat files do you usually find on a machine?

A. It depends on how much internet content is present.

Q. Do you believe that the size of an index.dat file ever changes?

A. It can, depending on the content of the index.dat. I mean, certainly, it can get bigger as content is added to it, but the behavior of Windows Internet Explorer is that, by default, four subfolders are created, content is leveled across each of those four subfolders as you increase your internet -- temporary internet cache, more folders are generated. I don't think it's accurate to say four index dot dat files are created.

Q. Would --

A. Those would be dependent on how much temporary internet content you have on your computer.

Q. Would it surprise you to find out that Microsoft specifies index.dat files remain static sized, notwithstanding content?

A. No, sir.

Q. How is it that those index.dat files are separated from one to another? What -- why are there different files?

A. Well, sir, there's index.dat files that pertain to daily history as well as weekly histories.

Q. And some of the index.dat files that are on the computer are -- that are on Mr. Cooper's computer, are for June, correct?

A. Yes, sir.

Q. They don't relate to any content in July at all?

A. That's correct.

Q. And yet, those index.dat files were modified at the exact same time as the other index.dat files on July 16th.

A. Again, the feed update, it would depend on where the content resides because the index.dat follows a particular subfolder. So, you know, if -- if there's an RSS feed associated with a particular day that's -- predates, you know, the content that's in July -- then I wouldn't expect that to be unusual for the index.dat from June, connected to one of these RSS feeds in June, to be updated when the RSS feed updater runs.

THE COURT: Might this be a good ---

MR. KURTZ: That'd be fine.

THE COURT: Okay. Members of the jury, it's a few

CONTINUED CROSS EXAMINATION

MR. KURTZ: Thank you, Your Honor.

BY MR. KURTZ:

Q. Officer Chappell, you knew it that we have alleged tampering with Mr. Cooper's computer?

A. Yes, sir.

Q. And your job is to investigate the computer, in particular, Mr. -- Mr. Cooper's computer isn't -- or your job to investigate that?

A. I suppose so, yes, sir.

Q. One way to verify whether something occurred on a computer at a certain time, particularly when it's over the internet, in addition to looking at cookie logs would be to look at router logs, correct?

A. I suppose that -- that's an accurate statement, assuming router logs exist.

Q. And probably safe to say that Cisco Systems, a company that makes routers, logs their router activity?

A. On their corporate network or on routers that they manufacture for consumers?

Q. On their corporate network.

A. I would -- I would assume so.

Q. You've heard testimony that, and it is your belief that, this took place while Mr. Cooper was in a Cisco building?

A. That's when that Google maps search artifact was created. He was connected to the Cisco wireless network access point called Blizzard.

Q. Okay. If Mr. Cooper was connected to Blizzard at that time and the web traffic was going through that Cisco network, there is at the very least a possibility that there would be router log information that could be obtained?

A. I suppose that's possible, yes, sir.

Q. Despite the fact that we've alleged tampering, no attempt has been made to get that router log?

A. Are you asking if I've attempted to?

Q. Have you recommended to anybody that they do that?

A. We've presented a number of pieces of information to the investigators in this case. I do not know what they have done with the information we've presented to them.

Q. Are you aware of any Cisco router logs that exist in this case?

A. We've not been given any -- any routers or any router logs to examine.

Q. You also looked at the master file table, the MFT?

A. I did.

Q. And, in doing so, you realized that all of the time stamps related to the internet artifacts from this map search, that all of them show an invalid timestamp in the standard attribute entry modified timestamp?

A. I'm not sure if every single one of them, but a number of them do. Yes, sir.

Q. Okay.

A. There's also a number of inaccurate file stamps on many other places on his computer that predate July.

Q. Okay. When you are unable to read a file stamp, did you attempt to parse it manually?

A. On a couple of occasions.

Q. Well, why did you not parse manually the file stamps that are important to this particular case?

A. The few that I tried, gave me an invalid results.

Q. So that -- it was not just a function of the tool that was used. The time stamp in itself, even when manually parsed, gave an invalid result.

A. On a couple of the ones that I tried. My conclusion was that that's a representation of either the tool or the operating system. I'm inclined at this point, based on some stuff we did last night for you, that it's an operating system defect of Vista.

Q. Okay. We'll -- we can talk a little more about the file system in -- in a little bit. In trying to figure out a cause, did you consider what Special Agent Johnson said yesterday about that timestamp showing as invalid because of placing material from something like a CD or an external source onto a computer?

A. I don't recall if -- if that was specifically his response or if it was in response to timestamps being out of order.

Q. It is true that placing a file onto a hard drive can render the standard information attribute entry modified to show as invalid; is it not?

A. I don't know that I would say that that's the only explanation for them.

Q. Not my question. Is it true that dropping a file from an external source onto a hard drive can cause an invalid timestamp in standard attributes entry modified?

A. It -- it may be possible.

Q. And even in your report, you -- you do acknowledge that it is possible to alter timestamps even down to the nanosecond?

A. I don't think I've said anything to that effect. To the nanosecond?

Q. Do you recall -- do you recall saying that, after talking about timestamp modification tools that you were only aware of altering things to the second, that it may be possible to calculate the file timestamps and place them into a file with a hex editor, but it would require painstaking effort for each single file?

A. I would say that's accurate.

Q. Okay. You're aware that, in addition to specific programs that are designed to alter timestamps, that it can also be simply scripted?

A. Assuming there is some things on the host machine that's creating those timestamps. Yes, sir.

Q. And that both the -- all eight of the timestamps can be altered using tools and or scripts?

A. I -- I would say that's a fairly broad statement. I don't know that all tools can modify all eight file stamps.

Q. Didn't say all tools. You are aware that there are tools that are capable of modifying all eight time stamps, both system information attributes and filename attribute?

A. I'm not aware of any specific ones, but I -- I'll take your word for it.

Q. You are aware that the security system that was running on Mr. -- Mr. Cooper's computer was CS Agent?

A. The Cisco Security agent, yes, sir.

Q. And, with that knowledge, did you checked the Cisco Security Agent logs?

A. Yes, sir. We -- we looked at those logs.

Q. And when you look at those logs, did you note that on multiple occasions there were inbound packets attempting to set up the machine as a server incoming on port 445?

A. I know there was a lot of traffic that was detected on port 445. And port 445 is used by Windows as a -- like a file sharing port. It's connected with SMB; it's called Samba. It's a port that's used when Windows machines on the same network communicate with each other, send files back and forth, things of that nature. But I'm also aware that all those log entries said that the activity was denied.

Q. Though you, in your own report, you talk about other situations where activity being denied can be a sign of somebody attempting to intrude upon a system?

A. I did, I think in the context of repeated password attempts, you would expect to see a number of denied entries for, like, a logon for example, like a number of the same entries for a logon where the password was incorrect, one right after another right after another, indicative to me, based on my training and experience of other intrusions that I've investigated, of like someone attempting to either do a brute force or a dictionary attack on a particular password.

Q. Similarly, when looking at the CS Agent logs, is it not indicative of an attempt to penetrate a system to have multiple attempts that are denied attempting to accept a connection as a server on a TCP port?

A. Which specific TCP port?

Q. From 445 -- from 10.48.76.54.

A. Okay. That particular IP address is an internal network address. It's a non-routable. It's not from the internet.

Q. And --

A. It's on the same network.

Q. -- if somebody had actually hacked into Mr. Cooper's wireless, that would mean that they were in fact on the same network?

A. It could also mean that the Cisco Security Agent detected something it did not recognize, and the default behavior is to deny something as potentially being malicious rather than to allow the connection to happen.

Q. But that wasn't the question. The question was, did that -- the fact that there is an attempt at penetrating the system that is actually from an internal IP address, could that be indicative of somebody who has penetrated the wireless network, at that point attempting to get into the individual machine?

A. Could you tell me which date that occurred on?

Q. July 15th.

A. Was it a single injury or were there multiple entries on that day?

Q. Three entries on that day.

A. Three entries simultaneously, one right after the other, three entries spread over a period of time?

Q. Three entries right after the other and then eventually process system recently communicated with the remote host and access to resource, which has caused the remote host to be marked untrusted.

A. That could be related to the Alterus software.

Q. It could be lots of things.

A. It could be.

Q. One of those things could be somebody inside the wireless network attempting to get into Mr. Cooper's computer; could it not?

A. That could be one explanation. There could also be a number of benign explanations.

Q. When was it that you looked into the CSA logs?

A. Last night.

Q. Why didn't you look into the CSA logs back when tampering was first alleged?

A. This was not the only case that I'm working on.

Q. When you checked for intrusion, did you check the hiber fill -- hiberfile, sorry.

A. The hiberfile.sys file?

Q. Yes.

A. That’s the hibernation file that's created if you have a computer that supports hibernation, sleep the computer, or actually power is removed, all the information that saved into this hiberfile.sys file that's essentially a snapshot of your -- your memory. And --

Q. And that can be a valuable forensic tool; can it not?

A. It -- it could be.

Q. It -- it stores everything that's in RAM at a certain moment.

A. At the moment the hibernation is -- is initiated. Yes, sir.

Q. Right. Then as a result of that, it's almost like a time machine in a sense. You can see what was on the machine at that moment in time.

A. Yes, sir.

Q. You know that time is an issue in this case.

A. Yes, sir.

Q. Did you look through the hiberfile.sys files in this case?

A. I didn't find anything that I felt was indicative of an intrusion.

Q. Did you look through them?

A. I -- I made a cursory look through a number of different files.

Q. Did you look through the hiberfile --

A. I --

Q. -- dot sys?

A. I think that was probably one of the files I looked at.

Q. Did you note what you were looking through and what you were finding as it happened?

A. I -- I don't make notes of negative findings.

Q. Did you look for restore points?

A. I did.

Q. Did you look through the Alterus logs?

A. I did last night.

Q. Have you time lined a combination of all the logs to create a master time line of computer activity?

A. Not of the Alterus or the CSA agent logs. I've looked at the Windows event logs.

Q. When time is in question in a forensic examination, is it not the best practice to integrate absolutely all of the logs into one master time line to look to ensure integrity of that time line?

A. Based on the time lines that I saw, I'm satisfied no intrusion had occurred.

Q. But you were not comparing or combining the logs into one master time line?

A. No, sir. I felt no need to do that.

Q. So if there was an entry at a certain time that conflicted with another entry for a file you had looked at days before, you would not have noted that since you weren't taking notes of the time and you never combined them into a single time line?

A. No, sir.

Q. Did you search for malware?

A. We did.

Q. And in your search for malware, did you ever look at the k-rundown file on this machine?

A. I'm not familiar with the k-rundown file.

Q. There are actually Vista system -- well, not just Vista -- there are files that occur in all kinds of different operating systems that malware essentially hijacks; is that a fair statement?

A. It -- a particular piece of malicious software can appear to be any kind of file, so, yes.

Q. But sometimes they actually hide themselves by using the name of a real system file.

A. In some cases it's a name similar to a system file, but using the name of a particular system file could -- could cause a problem.

Q. But in many cases, the intent is to cause a problem; is it not?

A. Well, depends on the particular malware and there's a lot of different things out there.

Q. Did you check the past signatures of the system files to ensure that none of them varied, so that all of them were what they appeared to be?

A. I checked all the files on his hard drive.

Q. And you did not note the -- that particular file as being -- as having a hash -- you did not note the k-rundown file not matching the hash of the genuine k-rundown file for Vista?

A. I didn't get any alert for any malware on the Defendant's computer over three different times that we ran it. We ran an initial assessment at that time that the exam was performed. We ran another one, I think, sometime around December of that year, and then we ran another one, I think, a couple months ago in connection with some sort of information that we had received from you. And in none of those three times did we get any sort of alert for any sort of malicious software, virus, Trojan, anything.

Q. Can you tell me what the significance of 178 Greenstone Lane is to the forensic evaluation of the computer?

A. It's not familiar to me.

Q. Okay. Are you able to tell from an e-mail header at what time the e-mail is read?

A. Assuming there's a read flag -- and by read I mean R-E-A-D -- that the message was read.

Q. Does the read flag actually tell you the time at which it was read?

A. Often times there will be a timestamp as far as when the event occurred of -- I'm not sure if you're talking about an e-mail header or specifically something related to Outlook and Outlook function.

Q. How can you tell when an e-mail is read, or can you?

A. If -- if there is an Outlook read flag that has been set because the message has been marked as read, then there's normally a timestamp associated with that.

Q. Looking at the e-mail headers yesterday, did you see timestamps associated with those e-mail read flags?

A. Which -- which e-mail header?

Q. Any of them.

A. I -- I don't recall specifically which e-mail headers you're referring to.

Q. How did you know that there was no MAC filtering on the Cooper system?

A. I don't. I still do not.

Q. Okay. Did you ever ask for access to the router?

A. I did not. No, sir.

Q. Is there a reason why you did not?

A. That was not something I was directly involved with.

Q. Would not -- wouldn't that have potentially given you information or insight as to what happened and at what time?

A. It would had I been the person involved with that aspect of this investigation.

Q. And who was the person involved in that aspect of this investigation?

A. I would say that the lead forensic examiner was Agent Johnson.

Q. I believe you stated that in order to access a computer you need a password in order to get into a user account.

A. That's correct.

Q. Isn't it accurate that there are readily available programs that will allow you to simply reboot and break into administrator accounts in -- in seconds?

A. There are boot CDs that would allow you to bypass a particular account password. Yes, sir.

Q. Another way of doing it is actually just to pull a hard drive and plug it in and access files?

A. Assuming you have administrative rights on the computer that you're using to view that hard drive, that could be correct.

Q. So if it's your computer and you take someone else's hard drive and you hook it up, you can look at that drive?

A. The drive that you're looking at, do you have administrative rights on your computer?

Q. It's on computer. If I have administrative rights on my own computer --

A. Uh-huh.

Q. -- I can view someone else's hard drive if I plug it in?

A. Potentially, yes, sir.

Q. I can modify data on that hard drive if I plug it in?

A. Potentially.

Q. You're aware that the registry entry for the BRACOOP user account was modified on July 16th; are you not?

A. Which specific registry entry?

MR. KURTZ: May I approach, Your Honor?

THE COURT: You may.

Q. Officer Chappell, I'm showing you what's been marked as Defendant's Exhibit 82, which has been previously identified as being the profile list registry report. If you would direct your attention to the highlighted portion, is that not a modification of the BRACOOP profile on July 16th?

A. It's a particular key of that profile. Yes, sir.

Q. And what are key properties of profiles?

A. Well, a key property is any key associated with a registry entry. There could be, you know, one or more keys of a particular registry entry.

Q. Thank you.

A. This was at 17:55 -- it's --

Q. Yes, sir.

A. -- UTC.

Q. Seventeen fifty-five UTC, which would be what time?

A. I believe that would be 1 p.m. -- 1:55? I forget the minutes. Is that --

Q. 1:55 p.m. on July 16th?

A. Right, and --

Q. And you are aware that Mr. Cooper was not in his house at that time?

A. Yes, sir. And I'm also aware his profile was logged into that computer, so if there was any service or process that was running under his login, it's not surprising to me that that profile key could have been updated; he was logged in.

Q. And in addition to that particular registry entry, you also note in your report, and we discussed it a little bit earlier, that invalid login attempts, particularly on an administrator account, can be a sign that someone is attempting to break into a computer.

A. Multiple, sequential, or a large number of repeated failed login attempts, yes, sir, I'd say that's consistent.

Q. And what you say in your report is, there was no entry in this log for any usual activity. We would expect to see failed login attempts if someone tried to guess or brute force user password on the system. If someone logged in as user BRACOOP on 7/16 when the computer was seized, there would have been an entry; there was not.

A. That's correct.

Q. You are aware, however, that on the 15th at 6:10 p.m., there was a failed login attempt on Mr. Cooper's administrator account?

A. 6:15 UTC?

Q. 6:15 eastern -- well, I guess it's daylight savings time.

MR. KURTZ: May I approach, Your Honor?

THE COURT: You may.

Q. Officer Chappell, I'm showing you what's been marked as Defendant's Exhibit 78, which contains the SIM user account registry entries. Does that actually specify that the -- the last attempt at a logon on the administrator account was on July 15th at 19:10 UTC?

A. Yes, sir, 7:10 UTC or 3:10 p.m. local time, 19:10 and 38 seconds UTC. It also indicates the last time the password was changed for the administrator account was on July 12th at 9:21 a.m. UTC, or 5:21 a.m. on July the 12th.

Q. Well, do you happen to have with you the list of logins that you had provided when it was Mr. Cooper was logged in?

A. I do not. I'm not sure if Agent Johnson might have brought a hard copy of that with him today.

Q. I believe that was entered into evidence and I may have a copy. I believe it's State's Exhibit 624. Now, I'm showing you State's Exhibit 624 previously admitted into evidence, the login summary report that was created for Mr. Cooper by yourself and Special Agent Johnson.

A. And what would you like me to look at?

Q. At what -- this lists a last password change time at what time?

A. On July the 12th at 9:21 and 14 seconds UTC, or 5:21 and 14 seconds local time on the 12th of July, and that's for the administrator account.

Q. Correct.

A. So what would you like me to look at?

Q. During that period of time, Mr. Cooper's computer was unlocked; is that correct?

A. No, sir. There's not a specific entry reflecting an unlock at 5:21 a.m.

Q. Because you're only showing when the screen is unlocked, not when it's logged onto?

A. When the actual event of control alt delete, and then the password is entered for the account.

Q. Okay. And the last written time for the administrator account, that was actually at, let's see, 3:10 in the afternoon, would you say?

A. I believe that would be correct, if converting UTC to local time.

Q. And at that point, Mr. Cooper was logged into his computer; was he not? Do you need the exhibit again? I'm --

A. I don't recall seeing specifically 3:10 p.m.

MR. KURTZ: Just a moment. May I approach, Your Honor?

THE COURT: You may.

A. So I'm looking at the 12th at what time?

Q. Looking at the 12th -- no, excuse me. Looking at the 15th at 3:10 in the afternoon.

A. Okay. There's a screen unlock at 2:05 p.m. There's a screen unlock at 3:35 p.m. Another screen unlock at 3:50 p.m.

Q. Are you able to tell from your activity logs whether Mr. Cooper was actually on the machine at 3:10 p.m.?

A. I'm not sure without looking at all the logs, but I'm assuming that he was logged into the machine at that time. Did -- did you have a question about that?

Q. Assuming he was logged into the account at that time, one would not expect to see administrator account access at the same time, would you?

A. I wouldn't say that's accurate. Windows allows secondary logins. Anyone who works on a corporate domain that has an IT department -- I don't know if you've ever had the occasion to have software or something installed while you're logged in, and administrator can do a secondary login. Windows supports multiple simultaneous user logins, so I wouldn't say that that's necessarily untoward, especially in light of the fact that when that administrator password was changed, it was at a date and time that the Defendant would have access to that computer exclusively.

Q. Are you aware as to whether or not Cisco had an administrator access at that time?

A. Again, not without looking at the logs to see what else was going on in the system at that specific time.

Q. But that is something that you could actually have found out from Cisco as well, correct?

A. That I personally could have found out or --

Q. That's correct.

A. I don't know that that would have been appropriate for me to find that out.

Q. Well, you said that it could have been --

A. A --

Q. -- external --

A. -- secondary login?

Q. -- that it could have been a secondary login. Isn't the last written time actually coupled with an SID unique identifier in the registry?

A. The last write time to a key?

Q. Yes.

A. The key has to be associated with something, so I would say, you know, the SID has to be present, the security identifier, so you know what account it's being written to.

Q. Wouldn't the SID unique identifier of 500 indicate local access?

A. I believe so.

Q. Were you able to find a BRACOOP password on the computer?

A. When you say a BRACOOP, do you mean a -- a password for his -- his account to log into that computer?

Q. Yes, sir.

A. There's cache credentials on his computer.

Q. Did you ever provide any information on cache credentials on his computer to the State or us?

A. No, sir. I don't see why the presence of cache credentials on a domain machine would be something that I would report.

Q. Well, you actually do list password entries on the report, do you not?

A. I list password entries?

Q. Or Special Agent Johnson?

A. I don't know. That's his report.

Q. And in what files were those credentials found?

A. In the registry, when a -- a computer is assigned to a domain, like a company computer, so in this particular case, this computer was joined to the Cisco domain and, in order to authenticate into a domain, you're authenticating normally across a network connection. Your computer's at your desk, plugged into your work internet connection. When you authenticate into your account, that authentication at your work desk takes place across the network to a domain controller. You supply your password, it compares that to what's on file for your user name. If the password matches -- and I'm kind of over-simplifying this a little bit -- and it says yes you're authorized to log in, you're able to log in.

Well, there are times where you're not physically connected to your work domain, if you take your laptop home, for example. So there has to be a way that you can still log into your computer and use it, and that's where cache credentials come into place. Would you like the specific registry key?

Q. I'd like the specific password.

A. I don't have the specific password, but the -- the key is located in the security hive under cache. There's by default 10 entries. The -- the only entry in this case is associated with the BRACOOP user account.

Q. But you did not feel it was something significant to note in any report?

A. The -- the presence of a standard Windows file being present on his computer?

Q. The password --

A. No, sir. I think that's irrelevant.

Q. The password itself.

A. Can you --

Q. Don't --

A. -- I guess, enlighten me as to why I would need to record what his account password is.

Q. Isn't it a relevant fact in a forensic investigation to determine the password and to provide that in the report when you write it up?

A. We're generally not in the practice of breaking an encrypted password. Looking at the hard drive with the forensic tools that we use, we can see everything on the computer. We don't log into the computer. There's no need for us to break the password, and --

Q. So --

A. -- I -- I do not believe I've -- I'm aware of an instance where the FBI provides passwords routinely in the course of us doing a forensic exam.

Q. Do you believe that information might be helpful for subsequent investigators actually following up on your work?

A. Do you mean investigators who don't have access to standard forensic tools?

Q. I mean subsequent investigators performing follow-up examinations -- law-enforcement, that they could access the machine live using a password. I mean, there are a multitude of reasons why I can see a password being relevant.

A. Any law enforcement examiner I'm aware of would not have a specific need to break the password. If it became necessary to, you know, make a copy of the hard drive and boot the computer up and work off of it live, I -- I suppose the password could be broken, but as a matter of course, we just don't do that.

Q. So you just see it as simply a irrelevant issue to -- to forensic examiners?

A. As I've testified, it's not a necessary thing that I need to have the account password in order to see any of the files on his computer.

MR. KURTZ: May I approach, Your Honor?

THE COURT: (Clears throat) Excuse me. Yes, you may.

MR. KURTZ: Thank you.

Q. Special Agent -- excuse me, Officer Chappell, do you recall performing an evaluation on Ms. Cooper's Macintosh?

A. I did.

Q. And this is, in fact, a copy of your -- your report on that Macintosh?

A. It appears to be. Yes, sir.

Q. And in that report, do you not state there were two user accounts on the computer? You list the create date?

MR. ZELLINGER: Your Honor, I object to this point. To what computer we're talking about? I think that needs to be cleared up.

THE COURT: Okay. I -- I thought he specified the Mac --

MR. KURTZ: I --

THE COURT: -- but he's talking about the Mac now, is my understanding based --

MR. ZELLINGER: -- Your Honor, that --

THE COURT: -- on his question.

MR. ZELLINGER: -- wasn't part of his question.

MR. KURTZ: Talking about the Macintosh.

BY MR. KURTZ:

Q. And in this report you say the password for account Brad Cooper was "nanner."

A. On the MacBook, yes, sir.

Q. In the password for the account Nancy Cooper was Bella123.

A. Yes, sir. That's because I performed the analysis on the MacBook.

Q. But yet your testimony moments ago was that you felt that the inclusion of passwords in a forensic examination was essentially irrelevant.

A. In -- in the context of the IBM ThinkPad. I did not perform the exclusive analysis of that. I did not write the report of the exclusive analysis of that.

Q. And do you recall yesterday going through a number of pieces of internet history from Mr. Cooper's machine?

A. On direct, yes, sir.

Q. And do you recall one of them was for Air Canada?

A. That sounds familiar. Yes, sir.

Q. Have you considered the potential that Mr. Cooper might have been looking to arrange for his parents to come down here?

A. I haven't considered the potential for why a -- a particular link to Air Canada is there. I merely stated there was internet artifact related to that particular website.

Q. Right.

A. It could be there for any number of reasons.

Q. And when you talk about internet artifacts that you find, one that you mentioned in specific, I guess, was celeb videos. You're aware that you don't have to be on a website to get an artifact like that; is that correct?

A. Yes, sir. I think I testified on direct that some of these cookies could be as a result of embedded ads on a particular web page.

Q. And you actually looked at the Citibank 1:14 -- web activity and noted that that was the web page hit at 1:14 in the afternoon on July 12th?

A. If that's when the net analysis says the last access was, that would be consistent.

Q. Did you note the fact that there was no logon to that account?

A. I don't have the logon right in front of --

Q. And you also noted that there was a search on Mr. Cooper's machine on July 13th for Edmonton that appeared to be a job search?

A. I think so, yes. That sounds correct.

Q. You -- you didn't mention at that time that the search was actually for a company called PSDN, did you?

A. If that was encoded within the URL, that's what I would have been talking about, the specific website.

Q. Were you aware that PSDN is Mr. Rentz's company?

A. No, sir.

Q. Did you note that the exact page that was accessed was the contact page for Mr. Rentz's company?

A. No, sir. I would have read whatever was being shown to me on the screen as the URL, as I did with many of those other entries.

Q. Do you believe that the answer that you provided to the question misleads people into believing that Mr. Cooper was somehow doing a job search, when he was actually considering a call to his father-in-law?

MR. ZELLINGER: Your Honor, I object to the characterization of misleading --

THE COURT: Sustained --

MR. ZELLINGER: -- especially --

THE COURT: -- as to --

MR. ZELLINGER: -- concerning --

THE COURT: -- the form of a question.

BY MR. KURTZ:

Q. Okay. Officer Chappell, I would like to go through the master file table entries, and particularly I would like to go through -- this is State's Exhibit 305. This is the master file table from that computer, which was previously admitted into evidence.

MR. ZELLINGER: Your Honor, I'd object to this point. The State's 305 is the laptop and -- and I'm fine if we're saying that everything on that computer is now in this one. If that's what the Defendant's saying, I'll withdraw my objection.

MR. KURTZ: Well, it's exactly what we've been arguing about.

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

BY MR. KURTZ:

Q. How many records exist in the master file table, Officer Johnson? If we could just scroll to the bottom?

A. My last name is Chappell.

Q. I'm sorry, Officer Chappell.

A. How many total entries?

Q. How many entries are there in the master file table?

A. One hundred sixty-nine thousand, two hundred and eighty.

Q. And now, of these entries, how many of them exist with an invalid timestamp?

A. Across all the various --

Q. Across -- through the system information attribute entry modified tab. Yeah, actually, first I'm going to hide the -- the extra columns unless there is some reason why they're relevant to you ---

A. It would be nice to be able to see the entire line if ---

Q. Okay.

A. -- we need to refer to something.

Q. Then -- then we won't -- won't hide them. If you could move a little bit further and go to the standard access entry modified, and if we could filter just so that we are only seeing those with invalid timestamps. Are you familiar with Excel, Officer Chappell?

A. Yes, sir.

Q. Would it be an accurate statement to say that if we select one column, it will give us the number of items in that column?

A. One column now that you've filtered everything?

Q. Well, actually ---

A. Well, you could also just go to the bottom of the column and do a formula that says sum above.

Q. Or if you look at the bottom left-hand corner, it says there are 3,349 records that filter as having invalid timestamps?

A. I think that -- that's accurate, yes.

Q. That's on the entire computer?

A. In that particular column, on the entire computer across all eight timestamps, there's 3,357 invalid timestamps.

Q. Asking you about this particular column --

A. And 3,349 in that specific column, that -- I think that's accurate.

Q. And what percentage of the file structure does that mean actually is invalid, for the entire computer?

A. Related to just those specific files or related to all the invalid timestamps? Because I've calculated for all 3,357. That would be 1.9831 percent of all the files. I haven't calculated just for that specific column, but it's fairly close. I mean, 3,349, 3,357 --

Q. So somewhere --

A. About two percent.

Q. -- about two percent. Just -- now, up until June 22nd, if we could limit the date range -- actually, I believe it won't let us drag up. Is it accurate that there are no invalid standard information entry modified in timestamps prior to June 23rd?

A. None that are reported as invalid. I'm not sure if there would be any. There is no timestamp reported and the field is blank. We did some testing last night. Some of the timestamp fields were also blank as well.

Q. The question is specific to timestamps that register as invalid, in the standard information attribute entry modified column.

MR. KURTZ: Now, if you would, if you could highlight from July 9th through July 12th, just one column.

Q. Now, these are still filtered files; is that accurate? We have not unfiltered the results?

A. I haven't seen you unfilter, so no.

Q. Can you make that determination by looking at the bottom number in the left hand corner that says 3,349?

A. Yes, sir.

Q. Okay. When it lists count on the bottom, slightly right of center, it says 2,621?

A. Two thousand, six hundred twenty-one. Yes, sir.

Q. Does that indicate that 2,621 of the files that bear standard information creation dates, out of a total number of 3349 files with invalid time stamps, that that is how many in that four-day span show as having invalid timestamps?

A. The column that you're in is the standard information creation date, and you're saying those files correspond to the standard information update -- the entry update?

Q. I'm saying that the files that are created from July 9th to July 12th contain 2,621 invalid timestamps.

A. It appears to, yes.

Q. Now, if -- do you know how many files were actually created during July 9th through July 12th?

A. No, sir.

Q. And what we're doing right here is sorting by the create date; is that accurate?

A. Appears to be.

Q. So, Officer, does that appear to be the first -- line 164162 would be the first of the July 9th time entry?

A. Yes, sir, it looks like it.

Q. Accurate that it shows a count of 3,627?

A. It appears to, yes, sir.

Q. Now, if 2,621 of them show invalid timestamps in that time frame, and that's what we just determined moments ago, is that not approximately 75 percent of the timestamps in that time frame showing as invalid?

MR. ZELLINGER: Your Honor, I'd object to the form of the question. What time frame?

MR. KURTZ: July 9th through July 12th.

THE COURT: Go ahead.

A. It would appear to be. I'll take your word on the math. They didn't tell me math would be involved today.

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

THE COURT: You may.

BY MR. KURTZ:

Q. Here's a calculator, Officer Chappell. Could you please tell me what percentage of the files show invalid timestamps from July 9th to July 12th, the number that you previously testified to as being inaccurate was 2621, and the total number is 3,627.

A. 72.263 percent. And, just so I'm clear, is this particular document, this output, is this the -- the output that we created or the output that your -- your expert, Mr. Ward, created? Because the -- was just noticing the fractional seconds are only three decimal places.

Q. I believe that this is the one that we created.

A. Uh-huh.

Q. I'm happy to go through it all with the one that y'all created, and I can also display further decimal points if you would prefer.

A. Well, I'm just -- I'm just not sure that -- I mean, there may be more, there may be a few less, but I mean it's -- there's -- I'm not going to dispute the fact that there's invalid file stamps all across multiple entries in the master file table.

Q. And finally, Officer Chappell, I'm going to take you to July 11th as the create date, to the precise time of the alleged Google map search. And we can highlight all of those files. At what time did the -- the search start?

A. Well, that depends. Is -- is that being displayed in UTC time, or is that being displayed in local time?

Q. It's being displayed in UTC.

A. So 5:14 I believe, because 1:14 would be the local time.

Q. Would that be the first one, as far as you can tell --

A. As --

Q. -- looking at it.

A. -- far as I can recollect, that -- that sounds correct.

Q. And it does bear the imprint that it's a MAPS file?

A. Yeah, the cascading style sheet, that would -- that would --

Q. Okay.

A. -- be accurate.

Q. And you can see in the far right corner, it shows the standard information entry date as having an invalid timestamp?

A. Yes, sir, it shows that.

Q. If we could scroll down until the end of the map search. There are 507 total files related to the search; is that accurate?

A. That sounds correct.

Q. And that would be the end of the search right there; would it not?

A. Show me the file name, please. And the -- the one right under it.

Q. Well, based on time, you can see that the one right under it is actually 30 minutes later, so you --

A. Okay.

Q. -- are able to eliminate that based on time, are you not?

A. Yes, sir.

Q. And based on every one of these entries, all 507 of them bear a timestamp in the standard information entry modified column as being an invalid timestamp.

A. In that one specific column. Yes, sir.

Q. And I'm sure you don't need the calculator. That's 100 percent, correct?

A. Yes, sir.

Q. Yet, on the remainder of the computer, the rate at which files appear to actually have invalid timestamps was approximately two percent.

A. That's accurate.

MR. KURTZ: I have nothing further.

THE COURT: Redirect.

MR. ZELLINGER: Can we leave that up there?

THE COURT: Please.

MR. ZELLINGER: Your Honor, can I approach the witness?

THE COURT: You may.