J. Andrew Coombs (SBN 123881)
andy@coombspc.com
Annie S. Wang (SBN 243027)
annie@coombspc.com
J. Andrew Coombs, A Prof. Corp.
517 E. Wilson Ave., Suite 202
Glendale, California 91206
Telephone: (818) 500-3200
Facsimile: (818) 500-3201

Attorneys for Plaintiff Louis Vuitton Malletier, S.A.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA (SAN JOSE)

Louis Vuitton Malletier, S.A., Plaintiff, v. Akanoc Solutions, Inc., et al. Defendants.	Case No. C 07 3952 JW (HRLx) REQUEST FOR LEAVE TO FILE MOTION FOR RECONSIDERATION OF ORDER RE: MOTIONS IN LIMINE; DECLARATION IN SUPPORT

Pursuant to Local Rule 7-9, Plaintiff Louis Vuitton Malletier, S.A. ("Plaintiff" or "Louis Vuitton") moves the Court for leave to file a "Motion for Reconsideration of Order Re: Motions in Limine" to address only the Court's ruling on Defendants' Motion in Limine No. 15 ("Defendants' Motion"). Docket No. 183.

This request is based on the fact the same order granted Defendants' leave to file their untimely motions in limine and Plaintiff was provided no opportunity to supplement the record or to dispute the positions adopted on behalf of Defendants. (Defendants' motion for leave, along with the putative Defendants' Motion was filed on Monday, the 6th and the order granting leave and simultaneously granting Defendants' Motion was filed Thursday, the 9th.).

Although Defendants' Motion was granted without prejudice, Plaintiff seeks clarification that opinions upon which the Plaintiff's expert was examined at deposition will be admitted.. Moreover, Defendants' Motion is predicated upon an incomplete account of the pertinent record, creating a misleading basis in support of their position.

Plaintiff easily meets its burden under Local Rule 7-9 and the Court's Order. At the time of this request, a material difference in the facts exists based upon Defendants' omission of several key facts, the Court did not consider material facts because they were purposefully omitted by Defendants, and Plaintiff was not given an opportunity to oppose Defendants' Motion at all.

I. Defendants Fail to Note They Were Given An Opportunity to Examine Plaintiff's Expert on All Relevant Opinions At His Deposition.

Plaintiff's expert, Michael Wilson ("Wilson") was examined at length on June 26, 2009. Among other things, Wilson was examined on documents produced to Defendants as part of Wilson's production pursuant to Defendants' deposition subpoena. These documents elaborated upon the opinion Wilson expressed in his initial report dated May 20, 2009, in which Wilson stated that he expected "to verify and authenticate the relevant portions of the ESI [Electronically Stored Information] collected by Mr. Murin." The documents produced before Wilson's deposition elaborated upon the contents of the ESI obtained as a result of the Court-ordered inspection first made available after Magistrate Judge Lloyd's order of May 12, 2009.

The Court will recall that the ESI was obtained after extensive objection, obstruction and motion practice dating back to Plaintiff's first request for production of documents propounded in November, 2007. When no documents were produced in response to Plaintiff's requests, the Court, after motion and objection by Defendants, ordered an inspection. Further motion practice was required to determine the protocol for inspection, a protocol that was not established until Magistrate Judge Lloyd's order of May 12, 2009. Plaintiff's expert accordingly had but eight days before the expert discovery cutoff to serve his report. This report was to address ESI evidencing staggering amounts of infringing material on but five of the servers maintained by Defendants, evidence which Defendants' themselves asserted was too voluminous in their Motion in Limine No. 12.

Notwithstanding this burden, an expert report was timely produced and supplemented, albeit just before Wilson's deposition was scheduled to begin. As no additional opinions have been

expressed by Wilson following the deposition, Plaintiff concludes that it is opinions included in the deposition should be admitted.

Moreover, Defendants did examine Wilson on the subject matter of those additional opinions. There is therefore no prejudice and exclusion of such evidence would be inappropriate.

II. Key Facts Were Omitted From Defendants' Moving Papers Resulting in a Materially, Misleading Timeline not Considered by the Court.

While Defendants' contend that they are prejudiced by Plaintiff's expert's testimony of which they were made aware prior to Plaintiff's expert's deposition and concerning which they deposed Plaintiff's expert, they do not mention in their papers that they produced their expert's supplemental report by email, at 6:02 p.m. the day before Plaintiff's expert's deposition. Declaration of J. Andrew Coombs ("Coombs Decl.") at ¶ 3. Plaintiff's expert could not have been expected to rebut those statements and provide his finalized supplemental report given only the night before his deposition.

III. Admission of the Opinions Will Expedite and Facilitate Resolution of the Issues Before the Court.

As noted above, the relevant ESI collected from Defendants' servers is massive. It evidences hundreds of websites incorporating offers of counterfeit merchandise infringing Plaintiff's intellectual properties as well as traffic logs indicating when these sites were active. Wilson's opinions will merely explain that data in a manner more readily understood by the jury, including presenting the data in the format in which it appeared when it was online, summarizing when the websites were active and Louis Vuitton offers were being accessed and otherwise providing a useful mechanism to understand the scope of the direct infringements abetted by Defendants on a mere handful of servers operated by them.

It is in the Court's own interest and considerably more efficient to permit introduction of the evidence in this format.

For these reasons, the Court should grant Plaintiff an opportunity to respond to Defendants' Motion through a Motion for Reconsideration in light of the incomplete representations and to prevent Defendants from gaining an unfair advantage at trial.

Dated: July 10, 2009

J. Andrew Coombs, A Professional Corp.

/s/ J. Andrew Coombs
By: J. Andrew Coombs
Annie S. Wang
Attorneys for Plaintiff Louis Vuitton Malletier, S.A.

DECLARATION OF J. ANDREW COOMBS

I, J. Andrew Coombs, declare as follows:

1. I am an attorney at law, duly admitted to practice before the Courts of the State of California and the United States District Court for the Northern District of California. I am counsel of record for Plaintiff, Louis Vuitton Malletier, S.A. ("Louis Vuitton") in an action styled *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., et al.*, and, except as otherwise expressly noted to the contrary, I have personal knowledge of the following facts.

2. On or about June 23, 2009, prior to the deposition of Mr. Michael Wilson, Plaintiff's designated expert, I sent correspondence to Mr. James Lowe, counsel for Defendants regarding Mr. Wilson's attempts to "rebuild" certain of the websites hosted on Defendants' servers. I received a response from Mr. Christopher Lai on that same date acknowledging my correspondence, and sent to Defendants' expert, a copy of the raw data from the servers that was delivered on June 24, 2009, pursuant to Defendants' counsel's instruction. Attached collectively as Exhibit A are true and correct copies of my correspondence to Mr. Lowe as well as the exchange between myself and Mr. Lai.

3. On or about June 25, 2009, Defendants submitted its expert's supplemental report by email at 6:02 p.m., which was also the day before Mr. Wilson's deposition. Attached hereto as Exhibit B is a true and correct copy of the email sent by Defendants' counsel after business hours on June 25, 2009.

4. On June 26, 2009, before the deposition of Mr. Wilson began, Mr. Wilson provided to Mr. Lowe additional documents and findings, including printouts from at least one "rebuild" as well as a draft of findings that were to be incorporated in his supplemental report, among other things. Mr. Lowe reviewed Mr. Wilson's documents and questioned him regarding those documents in great detail. Attached hereto as Exhibit C are true and correct sample excerpts from the working draft of the transcript of Mr. Wilson's deposition.

I declare under penalty of perjury that the foregoing is true and correct and this declaration was executed the 10th day of July, 2009 at Glendale, California.

_____/s/ J. Andrew Coombs_____
J. ANDREW COOMBS

EXHIBIT A

From: Andy Coombs [andy@coombspc.com]
Sent: Tuesday, June 23, 2009 3:14 PM
To: 'Lowe, James A.'
Cc: 'Annie Wang'
Subject: Akanoc Server Data

Jim

I understand that our expert, Mike Wilson is working with raw data copied from the servers at Defendants' location in order to attempt to "rebuild" certain of the websites hosted on those servers. In view of this, it may be that – as suggested by you during oral argument on Louis Vuitton's motion to modify the protocol – your expert will require access to the same raw data relied upon by Mr. Wilson. In anticipation of this, I have asked Guidance to make duplicate copy of the raw data. Please confirm that you do want this copy to be provided to Mr. Gralnik and, if so, how you would prefer the copy be delivered.

Andy Coombs

J. Andrew Coombs, A P.C.

517 East Wilson Ave., Suite 202

Glendale, CA 91206

Telephone: (818) 500-3200

Facsimile: (818) 500-3201

From: Andy Coombs [andy@coombspc.com]
Sent: Wednesday, June 24, 2009 10:13 AM
To: 'Christopher Lai'; 'Annie Wang'
Cc: 'Lowe, James A.'; 'Murray, Peggy A.'
Subject: RE: Managed Solutions adv. Vuitton, 10562.002, Akanoc Server Data

The hard drive will be sent out today.

Andy Coombs
J. Andrew Coombs, A P.C.
517 East Wilson Ave., Suite 202
Glendale, CA 91206
Telephone: (818) 500-3200
Facsimile: (818) 500-3201

From: Christopher Lai [mailto:CL@gauntlettlaw.com]
Sent: Wednesday, June 24, 2009 9:45 AM
To: Andy Coombs; Annie Wang
Cc: Lowe, James A.; Murray, Peggy A.
Subject: RE: Managed Solutions adv. Vuitton, 10562.002, Akanoc Server Data

Andy,

Yes, our expert wishes to receive a copy of the underlying data in the format in which it was obtained. Our expert would like the data to be produced on a hard drive similar to the hard drive that your expert produced to us earlier. The hard drive(s) can be sent to Richard Gralnik directly via whichever mail/logistics carrier that you prefer. His address is as follows:

Online Security, Inc.
5870 West Jefferson Boulevard, Suite A
Los Angeles, CA 90016

Chris

Christopher Lai, Esq.
Gauntlett & Associates
Tel: (949) 553-1010 ext. 256
Fax: (949) 553-2050
Email: CL@gauntlettlaw.com
Web: www.gauntlettlaw.com

From: Andy Coombs [mailto:andy@coombspc.com]
Sent: Wednesday, June 24, 2009 8:07 AM
To: Christopher Lai; 'Annie Wang'
Cc: Lowe, James A.; Murray, Peggy A.
Subject: RE: Managed Solutions adv. Vuitton, 10562.002, Akanoc Server Data

Your email does not appear to respond to our underlying question. Does your expert wish to receive a copy of the underlying data in the format in which it was obtained? If so, how would you like to have it delivered?

Andy Coombs
J. Andrew Coombs, A P.C.
517 East Wilson Ave., Suite 202
Glendale, CA 91206
Telephone: (818) 500-3200
Facsimile: (818) 500-3201

From: Christopher Lai [mailto:CL@gauntlettlaw.com]
Sent: Tuesday, June 23, 2009 6:40 PM
To: Andy Coombs; Annie Wang
Cc: Lowe, James A.; Murray, Peggy A.
Subject: Managed Solutions adv. Vuitton, 10562.002, Akanoc Server Data
Importance: High

Andy,

I am responding to your email to Jim regarding the method of producing, to our expert, the raw data that Mr. Wilson is relying upon in his attempt to "rebuild" websites.

(1) For data from Windows servers, our expert would like the data to be provided on hard drives with a Windows file hierarchy structure.

(2) For data from Linux servers, our expert would like both the data to be provided on hard drives and the actual version of Linux used by Mr. Wilson in attempting to perform his "rebuild."

(3) In addition, our expert would need to be provided with any extraneous tools, in installable versions, that Mr. Wilson uses or relies upon in performing his attempted "rebuild." Such items may include, but are not limited to, web server operating systems, programming languages used, webpage developer tools and programming language interpreters.

Chris

Christopher Lai, Esq.
Gauntlett & Associates
Tel: (949) 553-1010 ext. 256
Fax: (949) 553-2050
Email: CL@gauntlettlaw.com
Web: www.gauntlettlaw.com

EXHIBIT B

From: Murray, Peggy A. [PAM@gauntlettlaw.com]
Sent: Thursday, June 25, 2009 6:02 PM
To: andy@coombspc.com; annie@coombspc.com
Cc: Lowe, James A.; Brian S. Edwards; Christopher Lai
Subject: Managed Solutions adv. Vuitton (10562-002) - Supplemental Expert Report of Richard Gralnik
Attachments: Supplemental Expert Report of Richard Gralnik.PDF

Dear Counsel,

Please see attached Supplemental Expert Report of Richard Gralnik. Hard copy will follow via U.S. Mail.

Peggy A. Murray
Assistant to James A. Lowe, Esq.
Brian S. Edwards, Esq.
and Christopher Lai, Esq.
Gauntlett & Associates
Tel: (949) 553-1010
Fax: (949) 553-2050
Email: pam@gauntlettlaw.com

EXHIBIT C

□&k14H

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

LOUIS VUITTON MALLETIER, S.A., Plaintiff, vs. AKANOC SOLUTIONS, INC., et al., Defendants.	No. C 07-3952 JW (HRL)

Deposition of MICHAEL WILSON,

taken on behalf of Defendants at 517 E. Wilson Avenue, Suite 202, Glendale, California 91206, commencing at 10:00 a.m., Friday, June 26, 2009, before Mitch Genser, CSR No. 4239.

□

PERSONS PRESENT:

A Correct.

I also have the declaration of Joseph Murin and a screen shot that was taken by him of the CPRO database.

Then I have seven verification reports that show the evidence was acquired and verified correctly after acquisition.

And then I have the published paper that I wrote in order to get one of the certifications that I have.

And I have my CV. And I have this piece of paper which allows me to read off all that information.

Q So you're reading from a page that's been prepared that just lists what you've testified to?

A Correct.

And I also have what is effectively a rough draft for the supplementary report that I'll be writing concerning the information that I've been able to analyze so far. It's three pages of notes concerning what I found and basically how I found them.

Q What opinions do you intend to testify about at the trial of this case?

A I can't answer that fully because I don't know whether or not I will be asked to talk about more.

But at this point, my opinions will be the fact that the websites that I analyzed were online and accessible to

the outside world.

Q All of them?

A No, the websites that I analyzed.

Q I see.

A The servers were collected correctly. All of the images were fair and accurate representations of the servers on the day that they were collected. To the best of my knowledge, proper chain of custody and proper procedures were used during the imaging process.

And then I'll also be talking about what a normal hosting facility should be able to do in order to block website traffic.

I will also most likely talk about the fact that the websites for Akanoc and DEDI Web Host, which I believe are related, have a posted acceptable use policy, and I can go over what that acceptable use policy was according to their website.

I'll also talk a little bit about the screen shot that Joe Murin took during the imaging process that shows a number of instances where, according to the CPRO database, Akanoc, or Managed Solutions, took down websites because of counterfeit product-related activity.

Q Anything else?

A That's all I can think of at this time.

Q Are the opinions that you have just listed all indicated in your expert report and your rebuttal report?

A Sure. But one thing that I definitely want to clarify here is that Whois query is a generic term that has become used for any sort of search that

involves retrieving information about a domain name or an IP address. It's more than one type of query.

So saying that I did a Whois query on "X" doesn't necessarily mean the same thing as saying I did a Whois query on "Y." That's the important distinction here.

Q But you don't disagree with Mr. Gralnik that Whois information about a domain name can contain inaccurate information?

A Correct.

Q Is that partly because the information itself comes from a variety of sources and without necessarily the ability to confirm information?

A I wouldn't be able to tell you why it is. I can tell you that the information that you get when you do a domain name query isn't always correct.

Q It's been your experience?

A Yes.

Q I want to mark this three-page supplement, or whatever it is, as Exhibit 1558.

(Defendants' Exhibit 1558 was marked for identification by the Deposition Officer and is attached hereto.)

(Discussion held off the record.)

MR. LOWE: Back on the record.

116

Q Exhibit 1558 is what, please?
A It's basically a rough draft of the findings of my current analysis of the forensic images that were taken by Joseph Murin.
Q And those images are listed in the first section list right under the first paragraph?
A No. I did a cursory exam of all of the systems in all of the hard drives. So there are more than just what was listed here.
Q You said there were five systems, I thought. Did I misunderstand you?
A There are five systems. So yes, the five systems that I examined were these five.
Q That's what that list is?
A Yes.
And I examined the hard drives that came from those five systems. But I never actually saw those systems.
Q Those numbers beside the word "system" refer to what, as you understand it?
A The serial number.
Q Then the next part of this document says that you discovered a number of sites listed on the original 67 on the servers. And then you list some names that were either very similar or exact matches.

117

Then you have a list of several here.
Can you explain what that list is?
A Sure.
Of the original 67, I basically did a very simple search to get -- the easiest term to use is "low hanging fruit"; things that are very easy to spot and things that don't require a whole lot of effort to go find.
The results of that search were these websites.
Q What sort of search did you do for this initially?
A In this particular case, all I did was a keyword search on the directory names for the websites that were on the particular servers. It was very simple.
Q So you were looking for the names, for example, that are listed here by doing a key word search in the directory of the serves?
A Correct. I would look for Bag925, or Eshoes99, or Bigworld Shoes.
Q Okay.
A Of all of the systems that I looked at and all of the servers that I looked at and websites, these are the ones that popped up quickly and easily with no

effort on my part to find. It has nothing to do with whether or not the other 67 aren't there, it just has

to do with the fact that these were easy to spot.

Q So there are nine of them on this list; is that right?

A Yes.

Q Then you indicate further on that you then focused the rest of your time on bigworldshoes.com.

A Correct.

Q And the hard drive with the particular number, I'm trying to --

MR. COOMBS: I think it's the last four digits of the serial number.

THE DEPONENT: Correct.

Q BY MR. LOWE: That refers back up to this first list of things?

A No. It refers to the serial number of the hard drive itself. Well, you're right. It refers to that one, but not to the system.

Q So to back up to the top of this page, you have serial numbers of hard drives and the serial number of a system next to it?

A Correct. Well, actually, I have an EIN followed by a serial number of a hard drive and then the system that it was attached to. The EIN is the

evidence inventory number that Guidance assigns to it.

Q So the number 5924 is your shorthand for what's on the second line of this group up at the top of the page?

A Correct. It's just a way for me to figure

out which computer it originally came from.
Q And you used this last four digit process for all of them that you list here for the hit location?
A Correct.
Q So if I'm looking at this correctly, you found these particular nine hits on three different hard drives?
A Correct.
Q Now, where you're talking about focusing the rest of your time on bigworldshoes.com, you said that the website was running at the time the system image was taken. It had web logs to show access in general and to LV portions of the website.
Can you explain what you mean by that?
A Sure.
The system itself, when it was imaged, basically, for my forensic examination, I could determine that the website, bigworldshoes.com, was up and running at the time the system was imaged.
Q You could tell that how?

A We can get to that in a second, or it's up to you.
Q We'll wait.
A Okay.
And after getting some identifying information about the particular website, I found out where the web logs were. And I analyzed the web logs and found out that the website had been accessed up

until the time the system was shut down to be imaged. And the potentially LV portions of the website had also been accessed up until the time that the system was imaged.

Q What do you mean by "potentially LV portions"?

A I mean the portions that are listed on the website as being Luis Vuitton products. That's all.

Q Now, we're talking only about this one website; right?

A Correct.

Q So there were web logs that specifically related to LV products?

A For this particular website, there were web logs for the entire site. And then as it happened, portions of those web logs were easily identifiable as being from the LV portion. That's all. We'll get into

more detail if we go on.

Q Just for the record, what is a web log?

A A web log is a -- it would be a log that is created by the web server itself that tracks the connections made to a particular website. It tracks a number of different information points, but the major points would be the time that the access occurred, where it occurred from, and what it was accessing. There are other things in there, too, but those are the big ones.

Q So the next paragraph says that you used

LiveView .07b to create a virtual machine image of the forensic image previously collected.

Can you explain what that means?

A Sure.

First off, do you know what a virtual machine is compared to a physical machine?

Q Why don't you explain it for the record.

A When everybody thinks about a computer, they think about a physical system. They think about a box with a CPU in it and a hard drive and some sort of graphics card, et cetera. That is a physical computer.

The hardware can be different from computer to computer, but the process involved in using the computer is still generally the same.

The operating system interacts with the hardware at a level that is below where a normal end user is concerned and presents some sort of interface for the user to see and accomplish whatever tasks they're trying to accomplish.

The key part of this is that the operating system is what is concerned with paying attention to the hardware. The end user doesn't care at all what the hardware is. The only difference between the hardware is whether or not their game runs faster or slower or whether or not their picture loads quickly or slowly. Things like that.

A virtual machine is effectively the same thing, but there is one extra layer of abstraction.

The virtual machine application in this case, the program is called VMware. This program creates an abstraction layer between the physical hardware and the operating system. What this allows to happen is, the operating system can go on running and thinking that it's a full computer with its own CPU and its own hard drive and its own network card, et cetera, et cetera. But in reality, it's actually running on top of a base operating system on top of some sort of hardware.

What this allows the system administrator

or the end user to do is to take this particular virtual machine and move it from place to place without any concern at all about what sort of hardware it's running on, except for the minimal, the faster the hardware, the faster it runs type of deal.

So again, the reason why a VM machine is used or created is to allow portability.

In this particular instance, I didn't have access to that physical hardware that was running the image or running operating system that we took an image of. All I had access to was the operating system.

So what I did was, I used this program called LiveView to convert the forensic image -- or to convert a copy of the forensic image. The forensic image is still preserved without being modified in any way. It converts a copy of the forensic image into a virtual machine.

This allows me to pull up the virtual machine, to start the virtual machine as if it were an actual computer. I can start it in a window on my forensic system.

What this allows me to do is see the imaged system in the same way that an end user would have seen the original computer.

Q What do you mean by "end user"?

A In this case, an end user is literally whoever is using the computer in this case. So the end user would be whoever was sitting on the console, the end user would be whoever was logging in and looking at the website, anything.

In this case, I actually ended up -- once I converted the system to a virtual machine, I started up the system, changed a few network settings on my forensic system, and that allowed the virtual machine to act as if it were the actual web server that was imaged, including hosting all of the websites.

So by the time I was finished with this process, I was actually able to connect to the VM image and actually browse the websites that were running on the VM image at the time that the forensic copy was made.

Q To get back to my question, an end user would be someone who was actually viewing a website in your situation.

Is that right?

So no matter what, if you have physical access to a system, you can be the administrator of that system.

Q What extra work would that require?

A Well, the same amount of work that I needed to do in order to get administrative level access to the VM systems, which is, I needed to use a third-party application in order to reset the password for the administrator.

Q On the hard drives that you looked at, the systems that you were considering, was there a VM software on any of those, as far as you could see?

A I'm sorry. What do you mean?

Q Was there any virtual machine software available on those hard drives?

A You mean the virtual machine application, the thing that runs VM images?

Q Yes.

A No, not that I saw.

Q So of the five hard drives you looked at, there was no virtual machine software that would allow what you're talking about?

MR. COOMBS: Objection. Misstates prior testimony; vague and ambiguous.

THE DEPONENT: I'm sorry. I don't

understand that one.

MR. LOWE: I'll try it again.

I'm just trying to clarify what's there and what isn't there.

Q In order for you to do what you did, you had to attach the hard drive to another computer, your own forensic computer, I believe you called it.

Is that right?

A I didn't have to attach the hard drive, I needed to have the forensic image of the hard drive.

Q And was that a hard drive, or was it in some other physical form?

A It was the forensic image. Remember the EnCase evidence files that we were talking about earlier?

Q Okay.

A All I needed in order to do this was the EnCase evidence file.

Q So you didn't actually plug in the hard drive to the computer you were using?

A Correct; I had the forensic image of the hard drive.

Q So you were running it through the EnCase system on your machine?

A Correct.

Q But also on your machine you had a virtual machine or VMware installed?

A Correct.

Q So my question is, did you see any evidence

that VMware was installed on the hard drives that you were examining?

A No. But it doesn't need to be.

Q Why doesn't it? Where else would it be if it's not on the hard drives?

A The VM application, which is called VMware, VMware Work Station 5.55, I believe. That's the application that is actually used in order to run virtual machines. That application reads a number of files that effectively is the virtual machine, or the virtual machines, plural. And it uses those files to recreate the operating system and to recreate the virtual computer.

Q But my question is, where is that application, VMware; where is it installed?

A That's what I'm trying to get to.

I have my forensic system, which is a physical computer. On my forensic system, the VMware Work Station application is running. And inside that VMware Work Station application is the virtual machine that was created out of the hard drive from the web

server that was imaged at Akanoc. So that's the layers that we're talking about here.

So there was no VM-related software installed on the VM system itself. The VM system is, for all regular purposes, exactly the same as it was when it was running on the systems at Akanoc.

Q But my question is, the VM software is

something you were actually using for your analysis?
A Yes.
Q Where was that VM software installed?
A On my forensic system.
Q Okay.
Was VM software installed on the hard drives that were taken from the copies of which were taken from Akanoc and Managed Solutions?
A I didn't actually check, but no, not that I could see.
Q You have no evidence that that would be on there?
A No.
Q But you would need to have VM software in order to do the kind of analysis and viewing of the system that you did without administrator passwords?
MR. COOMBS: I think he was fine until you added the "without administrative passwords."

THE DEPONENT: Right.
Q BY MR. LOWE: Does the VM software allow you to get around any password protection on the hard drive?
A No, it does not.
Q So how did you get around passwords?
A There are a number of applications that are designed for resetting administrative passwords. There are lots of different uses for them. Predominantly, the uses are because you administer a system and you forgot what the administrator password is.

A You would have some sort of management console at the firmware level of the system itself that would allow you to reset the passwords remotely through some sort of console access.

Q How do you know that?

A Because I've done it in the past.

Q You've done that with your own systems?

A Yes.

Q Do you know if that facility was installed on any of the systems at Akanoc or Managed Solutions?

A No, not without looking over the testimony again. I believe that that's what he was talking about,

but I don't remember.

Q You also talked about LiveView .07b?

A Yes.

Q What is that?

A LiveView is the application that you use to convert an image of a system, or a hard drive, if you happen to have a physical hard drive, to create a VM, a virtual machine image, of that physical image.

So LiveView does is change the -- or adds some extra information to allow you to boot up the system as a VM system. That's all it does.

Q Once again, LiveView was not installed on any of the hard drives or systems that you were inspecting?

A Right, nor did it need to be.

Q It was needed, however, for you to do what

you were doing?

A Correct.

Q Correct me if I'm wrong, but I think your testimony is that in order to do what you did to look at the directory of these hard drives, you had to have the EnCase software with the data from the hard drives on it; you had to have VMware; you had to have LiveView; and you had to have a password resetting program.

Is that correct?

A In order to view the information in the forensic image as if it were a live system, I needed all of those things. In order to view the information, all I need is an application that will read an EnCase evidence file.

So the data is still available off the forensic image in a pristine and unchangeable state. But in order to see it in the same format that a user would see it, you need all of these other things.

Q And I presume that you didn't find EnCase installed on any of these systems?

A I would hope not, no.

Q That's a specialized piece of software that forensic examiners use?

A Correct.

Q I guess it's also kind of expensive?

A Relatively, yes.

Q How much, just roughly speaking?

A I believe it's around $5,000 for a single

Q So under those circumstances, you would essentially have to have the consent of the customer to do the sort of viewing that you're talking about?

A No. "Consent" implies that you need their permission ahead of time, and you certainly don't.

Q What do you mean, "you certainly don't"?

A I mean, you don't need the permission of the person who is controlling the system in order to reset the password.

Q Okay.

A It may irritate them, but you don't need their permission ahead of time. You do not need their consent to do any of these steps.

Q But they would obviously know about it if you did some of these things?

A Most likely.

Q Down at the bottom of the first page on Exhibit 1558, you have a series of things that are called "server stats." Are we talking here about the server concerning bigworldshoes.com?

A Yes, we are.

Q And only that?

A Correct.

Q So you list the operating system, the physical components of the system, the hard drives, and so on; right?

A Yes. It lists the operating system and the fact that there were two hard drives in the system.

Q Are we talking about two physical hard drives or two logical drives?

A Two physical hard drives.

Q And which one was imaged?

A Both were imaged.

Q Is that reflected anywhere in the notes that were taken by Mr. Murin?

A Yes.

Q One of the hard drives you indicate hadn't been running as a primary operating system since January 15, 2009; correct?

A Correct.

Q And what does that mean, if anything?

A That means that the operating system on the hard drive with the last four digits of 4830 showed indications, after a short forensic analysis, that it had been a primary operating system on or around January 15th. There was access to the hard drive after that, but there wasn't access to the hard drive in such a way that would indicate that it was actually running

as an operating system. So it was probably in the system as a secondary drive.

Q Item 3 at the top of the second page says, "328 running IIS V6 websites."

What does that mean?

A There were 328 IIS Version 6 websites running on that system at the time that it was imaged.

Q And IIS Version 6 is what?

A Version 6 is the version of internet information server service, the web server.

Q So this is your term for -- or maybe it's the official name -- of a program of a web server that you've talked about before?

A Correct.

Q Do you know who installed that system on there? Is there any way of telling?

A There is a way. Well, there is not a way of telling the physical person who installed it, but there was a way of telling when it was installed.

Q Did you determine that?

A No.

Q But some kind of a program like that would be necessary to operate a computer as a web server?

A Correct.

Q Then the next portion of this information

D

talks about what you call "Findings concerning the website itself." And once again, we're talking about bigworldshoes.com?

A Yes.

Q Can you go through what you listed here. It appears to be written in language other than English. Perhaps you can help us understand what you're saying.

A Certainly.

Again, these are rough draft notes for the report, so it's written in what would be easiest to say as technical shorthand.

So what I found about the particular website itself was, it was running as of the date that the system was actually imaged, which was March 25th, 2009.

The logs for this particular web server are kept at that location listed ending in w3svc16.

The home directory was at that location listed, which has "bigworldshoes_com" in the name.

It was running on that particular IP. I can read it if you need me to.

Q No.

A The web logs show that the website was being accessed up to the date that it was imaged, which was March 25th.

Also, after examining the website itself and

the logs, a large portion of the Luis Vuitton-related products appeared to have had pictures that were located in a directory with that designation, "THY=."

So basically, the pictures were in a subdirectory somewhere after that point.

Q Okay.

A Also, the main page for the LV products had a URL that ended in "pcid=16." So what I did was, I analyzed the web logs for the entire website as it stood and specifically just for those two items. And again, what I was able to determine was, the website was running, accessible, and accessed at least between January 31st and March 25th of 2009.

Q Okay.

A The only other part is Number 8. The LV-related pages on the website were accessed at least between February 27th and March 25th of 2009.

Q Okay.

The web logs that you looked at, are they publicly available to the user?

A No. They shouldn't be.

Q Typically, web logs are not available to someone viewing a website?

A Not unless the website is configured incorrectly, yes.

Q By that you mean that someone who is running a website does not want someone to look at the web logs normally?

MR. COOMBS: Calls for speculation.

THE DEPONENT: I'm not sure that they would care one way or another, but it is usually extraneous data that doesn't matter. It's usually back-end tracking sort of data that wouldn't be publicly available.

Q BY MR. LOWE: And if you did see it on a website, you would think, as you said, that someone had configured things incorrectly?

A Yes, I would.

Q You then accessed some images or something from this directory THY=.

Is that right?

A Which one are we talking about?

Q For example, Number 6. You said, "I noticed that a large portion of the LV-related products had pictures in the directory 'THY=.'"

A Yes.

Q It says, "So I extracted hits with text 'THY=' in them."

What do you mean by that, "extracting hits"?

A I mean that the web logs were certainly over

100 megs' worth of text data, so screens and screens and screens of information. Within all of that information, there were hits that specifically dealt with pictures within the THY directory.

So what I did was, I basically filtered for only those hits and put those into a separate file and then analyzed just those hits.

Q And you were not viewing those files through the website main page, for example?

MR. COOMBS: Objection; ambiguous.

THE DEPONENT: Actually, yes, I was, at least at one point. By the time I had the whole thing rebuilt and visible, yes, I could actually access the website as it had been visible at the time the system was imaged. So I could access all of that information to verify that they all came from roughly the THY directory.

MR. LOWE: Well, I guess I'm just not clear as to what you were doing here.

You say you extracted hits with this text in

them.

Q What do you mean by that? You said, if I remember correctly, that you looked for those file extensions, or something in that directory, and you put that in a separate file.

146

Is that right?

A The easiest way to describe it would be -- well, let's take the expert report from Richard Gralnik as an example.

If you wanted to only find lines in it that had the word "domain" in them, you would do a search for the word "domain." And every line that had "domain" in it, you would then extract or set aside or move or copy, or whatever, and put all of those into a smaller, preferably less than 48-page document that just has "domain" in them. And then you could analyze each line that had the word "domain" in it.

That's the same thing that I did with these particular web logs, so any web log line, any entry that actually had "THY=" or "pcid=16" in it.

And I extracted those out of the larger set of data and put that in one file, a significantly smaller file, so that I could then analyze just that information.

Q And how large was the file that you were searching, or the files?

A That's the web logs that I provided on the CD that would have been voluminous. Like I said, they

had web hits from January 31st to March 25th on the order of thousands.

147

Q Thousands of hits?
A Many more than thousands of hits, thousands of pages. You're getting into an area that I can very easily describe for a very long period of time, but you don't want me to.
Q I'm just trying to get an understanding of the size of the data that you were searching.
A Honestly, the easiest way to do that would be to either wait for my final report or take a quick look at the CD and see how big it is; it's very large.
Q Did you measure it? Do you have any estimate in terms of megabytes, gigabytes, terabytes, whatever?
A It would be multiple megabytes, but probably not gigabytes worth of data.
MR. COOMBS: Just for the one website?
THE DEPONENT: Yes, just for the one website.
Q BY MR. LOWE: So the hits you're talking about came from the web logs?
A Correct.
Q The images came from where?
A The images came from the home directory or came from a subdirectory of "bigworldshoes_com/htdocs," which is basically the website location.

148

Q Is there a file in that system that just had pictures in it?
A There are multiple pictures. There are actually very many directories that just have pictures in them. One of those directories has primarily pictures of LV-related products in it.
Q One of roughly how many directories?
A I actually cannot tell you at this point.
Q Thousands?
A Hundreds.
Q You were starting to say earlier, I think, that you rebuilt the system somehow. I'm not sure I understood what you were talking about.
A That would be the LiveView thing where I converted a copy of the forensic image into a VM so that I could boot up the system as it would be a normal computer.
Q So is that the way you then access these pictures, or not?
A I access the pictures both through the VM image and through the forensic image itself.
Q I'm not sure I understand the distinction you're making.
A The major distinction here is that the forensic image itself is "read only." So any of the

data in the forensic image is pristine, is not touched,

is not changed in any way. So if I want to do any sort of comparison for file access times or any sort of MetaData, I have to do that through the forensic image.

Q That's not quite what I was trying to focus on.

When you were looking at or determining the content of the pictures, the photographs, were you doing that as if you were viewing the website as an end user, or were you doing it in some other fashion?

MR. COOMBS: Asked and answered.

THE DEPONENT: I was doing it both ways. I was doing it as I was viewing the website, and I also viewed them through the forensic image.

MR. LOWE: I guess I don't understand what you're saying by you "viewed them through the forensic image."

You identified certain directories because of information you got from the web logs that had, for example, LV images in them, I think you called them.

Q Is that right?

A Yes.

Q And then did you directly access those images in some fashion other than looking at it through a web page?

A Yes, I did.

Q And how did you do that?

A That was directly through EnCase and looking at the forensic image that was originally acquired.

So what I'm trying to say is, I did both. I didn't just rely on the rebuilt VM system. I looked at the data as it would have been visible by a normal user through the VM system, and then I verified the data's location and content and made sure that everything was exactly where I expected it to be on the "read only" forensic image that is an exact duplicate of the system that was imaged by Joe.

Q So when you were looking at it through the forensic image, as you've called it --

A Yes.

Q -- you accessed the directory specifically; is that right?

A Yes.

Q Were all of the LV images, as you've characterized them, available through a web page of bigworldshoes.com, as you had reconstructed it?

A I wouldn't be able to tell you if all of them were visible or not. All I saw was a sampling of the files.

Q So you saw some that way?

A Yes.

Q And then you just went directly to the directory to look at more?

A Correct.

Q Still on page 2 of Exhibit 1558, item 9 says, "I processed the logs using Webalizer."

What is that?

A Webalizer is a free tool used for processing web logs to give a graphic representation of access to a website.

Q Is Webalizer something that is typically installed on a website, or is it used by an administrator or somebody?

A It's used by an administrator. And actually, it's a relatively common program because it's free.

Q Well, there are a lot of free programs.

A It's a relatively common program because it's free, and it actually does a decent job at what it says it's doing.

Q Tell me more about Webalizer and what that process is that you did.

A Webalizer is, as I mentioned before, an application used for processing web logs to give the user some sort of graphical or statistical information

as to traffic to a particular website.

It can be used for all sorts of different reasons, sometimes just for curiosity and sometimes for billing purposes; it really kind of depends. But the bottom line is, it will take web logs and parse through them in some sort of reasonably intelligent manner, and then compile that information into a human readable and understandable form.

Q Generate some reports?

A Yes.

Q And you generated some reports for yourself?
A I did.
Q And you have them there in front of you?
A I do.
Q Might I see them?
A Yes.
Q You were about to say that they're on this disk?
A Yes, they're on a disk. And they're actually easier to read on that disk than they are on the printouts.
Q For the deposition, we need paper.
(Discussion held off the record.)
MR. LOWE: Back on the record.
Let me ask you a couple other questions

while we're waiting for the copies.
Q A little further down, about the middle of the second page, you indicate, "There is an extremely similar website currently online," and you have the particular IP address.
A Yes.
Q It's a different IP address than had been running previously; is that right?
A That is correct.
Q So what you mean to say is that you found bigworldshoes.com at another IP address?
A Correct.
Q And when was that?

A Yesterday.
Q And what does that mean to you, if anything?
A It just means that the website that is currently on the forensic image is effectively the same website with updates as the one that's running somewhere else right now. That's all.
Q Do you know where it's running?
A I know that it's not running at Managed Solutions, but I don't remember where.
Q So this IP address is not one assigned to Managed Solutions or Akanoc?
A Correct.

Q Then the next sentence says, "After 'slurping' the online website using HTTrack, I did a comparison," et cetera.
What is "slurping"?
A "Slurping" is kind of an industry slang. And effectively what it means is downloading a website in its entirety through the actual user interface. So HTTrack is a program that just automatically does that. So what it does is, it "slurps" all of the available links and all of the available pictures and all of the code that it can actually see and pulls it all down and does its best estimate in recreating the actual directory structure and puts it all on your system so that you can browse a website offline.
In this case, I used it to grab as much of the website as I could in the time that I had just to

compare the two sites together.

Q Does it grab only publicly available information?

A Yes.

Q So it doesn't grab, for example, web logs?

A No, not unless it's publicly available.

Q So if I understand the rest of this paragraph, you said that it was substantially similar to what you saw on the collected hard drive image?

A Correct.

MR. LOWE: I'm going to mark a copy of this as Exhibit 1559.

(Defendants' Exhibit 1559 was marked for identification by the Deposition Officer and is attached hereto.)

Q BY MR. LOWE: Exhibit 1559 is what, this group of documents?

A Exhibit 1559 is the printed out PDF'd Webalizer web pages. So it is the result of the web log analysis that is exported by Webalizer.

Q Would you agree that it's far more information than anyone really wants to read?

MR. COOMBS: Calls for a speculation. Speak for yourself.

THE DEPONENT: In my opinion, there is significantly more information than is readily usable to a layman.

Q BY MR. LOWE: We'll try a few pieces of it

here?

A Okay.

Q The first page looks like a summary of hits from February 2009. You mean people actually visiting the website. Is that it?

A Yes. Well, there is a difference between

people visiting a website and hits, unfortunately. Back when websites were first made, it was one static HTML page. And pretty much every time there was access to that one web page, it was one person clicking on it.

Unfortunately -- or fortunately, depending on your point of view -- nowadays websites and web pages have significantly more than one item on them. What that means is, a web page that looks like bigworldshoes.com could have 5 or 6 or 10 or 20 different items available on it. That means that every time somebody looks at it, it could be 5 or 6 or 10 or 20 hits. So it's not necessarily a one-to-one ratio between hits and pages or hits and visits, or things like that.

So what I can tell you is, the total number of hits is the total number of items that were touched during this time frame.

Q On this first page, during February of 2009, it looks like the total visits were four, and the total hits were 63.

Is that correct?

A That is what Webalizer thinks, yes.

Q Do you think that's correct, or is there some reason to doubt it?

A I think that the total hits is correct.

I happen to not necessarily agree with Webalizer's idea of visits. But I'm also generally not concerned with visits.

Q What is your understanding of the phrase "Total Unique URLs"?

A "Total Unique URLs" should be the -- it should be how many unique URLs were actually touched during that time frame.

Q URLs within the website?

A Yes, URLs in general, but URLs within the web logs.

Q The next page shows a couple of graphs. What roughly do they show?

A Basically, they show a graphical representation of the information on the first page, which is that there were 63 hits during February.

Q And the dates when those happened?

A Exactly.

Q It looks like it only had a couple of days of activity.

Am I reading that right?

A Yes.

Q I'd like to move to a page that's marked as "6 of 6," but it has a pie chart on it.

A Yes.

158

Q And it looks like this is entitled "Usage by Country for February 2009."
A Yes.
Q And do I understand that 97 percent of the -- is that visits or hits? It looks like hits.
A I believe this is hits, yes.
Q -- were unresolved or unknown; is that right?
A Yes.
Q What does that mean?
A Well, this just means that my computer that isn't connected to the Internet couldn't do any sort of resolution on the IP addresses that hit the -- the IP addresses that were responsible for these particular hits. It doesn't necessarily mean that they all wouldn't be resolved on a system that could actually go out and look. But for security purposes and for the preservation of evidence and all that, my system doesn't have direct Internet access. So it couldn't go and try and resolve any of these things.
Q So it had to look only at the data that you had been able to pull off the hard drive?
A Correct. And some sort of internal cache. And probably the internal cache is where it got the fact that some of these were from France.

159

Q So 3 percent of the hits were from France in February of '09?
A Correct.
Q And the others you don't know?
A Right.
Q Then it looks like the next page goes on to the last 12 months.
A Yes.
Q So I guess we're talking from June 2008 through June 2009?
A I believe we're actually talking about April 2008 through March 31st of 2009.
Q Once again, it's showing hits and visits; right?
A Yes. It's showing 79 hits in March and 31 hits in February. Actually, I'm wrong. That was the daily average.
It's showing 1,903 hits in March and 63 hits in February. So significantly more in March.
Q The next page shows just March hits, or hits and visits; right, March 2009?
A Correct.
Q The next page after this and some others in here have a set of information called "Daily Statistics." And it lists things by day. And many of

these are expressed in percentages. That's a percentage of what; do you know?

A It would be a percentage of the total in that particular column.

Q A few pages further along, it looks like there is a pie chart for March of 2009, Usage by Country.

A Correct.

Q And aside from the unresolved and unknowns, it looks like the hits came from Canada, France, China, Switzerland, Germany, India, and Hong Kong.

Is that right?

A Correct.

Q The next page is -- I'm not sure how this differs from the first page we looked at; it looks like February of '09.

A The first section was just the LV-related hits.

Q Okay.

A The second section is the entire website.

Q So starting at this page, about halfway through, is everything?

A Correct.

Q Going back to the first page, is that what the "THY" and the "pcid=16" refers to?

A Correct.

I was in a hurry. Probably it would be better to have them switched.

Q Going on to the next pie chart. It looks like February of 2009 again. Most of them, 92 percent,

are unresolved, but Canada and China are listed as sources of hits; right?

A Right.

Q Actually, there are a couple of others: Netherlands, Antilles, and Great Britain.

A Correct.

The next chunk of data is for the 12-month period.

Q Starting where? Is it headed, "Statistics for bigworldshoes.com"?

A Yes. And then the next line says, "Summary Period: Last 12 Months."

Q Maybe I'm on the wrong page. Okay.

And the page after that looks like "Summary Period: January 2009."

Is that right?

A Correct.

Q And the next page has to do with January '09?

A Yes.

Q And the next pie chart is January '09; is that correct?

A Correct. That's January of '09 for the entire website, bigworldshoes.com.

Q So it looks like 31 percent are unresolved and other countries are listed: Netherlands, Great Britain, Belgium, Brazil, Italy, and China; correct?

A Correct.

Q And then the last page is yet another pie chart.
A Yes.
Q For March of '09?
A Correct.
Q And this is, once again, for all of the website, bigworldshoes.com?
A Correct.
Q And it reflects that 70 percent are unresolved sources of hits, and the others that were reflected are China, Canada, and France?
A Correct.
Q So at this point in time, you have only reviewed information for this one website, bigworldshoes.com?
A Not quite. At this point in time, I have done what I would consider to be a relatively in-depth

analysis of this one Website. I've done cursory examinations of a number of different websites.
Q But you don't have the same amount of information on those others?
A Correct. I can get it, though.
Q What do you have in hand today?
A Just for this website.
Q In the middle of page 2 of Exhibit 1558, under your "Collection Findings," Number 2, perhaps you could interpret that for us, "TTBOMK."
A "To the best of my knowledge."