

Subject: Fwd: Additional Questions on your Daubert Analysis

From: JGross <JGross@tgplaw.com>

Date: Tue, 20 Jan 2015 19:13:10 +0000

To: Cottom Kirk <kcot@lle.rochester.edu>

Kirk,

Below is the reply by Dr. Podhradsky to your email. I talked with her about the reply and whether your email causes her to change any opinions in her report even to the slightest and the answer is no.

Thus, there is no legal basis for a Daubert motion or to challenge to the NIT.

So, if I continue as your attorney I intend to file a motion to withdraw the previously filed Daubert motion but not until Judge Bataillon hears and decides my motion to withdraw. Until he makes a decision whether I will continue as your attorney, I do not have any authority to act on your behalf as your attorney.

I understand you will not agree with my position on the Daubert but I have the report of three experts in academia with excellent qualifications and all agree there is no basis for a challenge. So, this is a final decision for me.

Reply with questions or thoughts.

jfg

Joseph F Gross Jr

669 North 57 Street

Omaha, Nebraska 68132

402.850.5245

Begin forwarded message:

From: "Podhradsky, Ashley" <Ashley.Podhradsky@dsu.edu>

Date: January 19, 2015 at 4:03:34 PM CST

To: JGross <jgross@tgplaw.com>

Subject: FW: Additional Questions on your Daubert Analysis

Hi Joe-

Our response to the questions are below. Some questions were outside of our scope, but we could look at them if needed. Some questions would be better answered with a look at his computer. Please let us know how you want us to proceed. Basically, there are always different ways to approach things and analyze data. We didn't have the entire package here without his computer, but our final opinion probably wouldn't change much given we are confident with our first analysis.

Step 1: Does the NIT meet NIST Standards? My three questions for Ashley's team for this step are:

1) Repeatability: Can you obtain the same results when using the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time? (Ashley's crew appears to have answered yes to this question with regards to the front end, but they did no tests on the back end. HD Moore, the methods author notes, "Without knowing how the backend was written and how the session IDs were generated, it is hard to say how reliable this system is. If they implemented something similar to the original Decloak demo server, it should be fairly reliable in terms of linking a proxy IP with the IP behind it." Ashley's team didn't test the back end at all so I don't understand how

A) Ashley's Team doesn't answer this question.

4) Do Standards Exist for the control of the techniques operation?

We don't understand what he is asking

A) Ashley's team doesn't answer this question.

5) Has the method received general acceptance in the relevant scientific community.

A) No for the NIT itself, Yes for the ability of a Flash app to "decloak" Tor clients.

The establishment of a TCP connection and sending data is well accepted in this field.

Federal courts are unanimous in holding that computer evidence generated by or resulting from a process is only admissible if the defense has access to such software in order to independently duplicate the results of that process and thus "is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence." I don't understand why only half of the NIT was tested. And that half was tested using reverse engineering instead of the actual Actionscript and Javascript.

It is possible that the FBI could have added extra code into the NIT and if we did not RE it, we could have missed something.

If they would provide the source that they used we could have compiled the flash app ourselves, we were under the impression that was not available to us as we asked in advance for the source.

As I pointed out in my other note, the NIT is high customized software with a relatively simple front end and a much more complex back end that is still a mystery.

Plus I have 6 more questions:

1) Could the half of the NIT they tested be injected into an iframe at an exit node causing the browser to secretly load the two pages in question?

It's possible but that would be a very targeted attack. If the connection was over SSL/TLS than it would not be possible so it also depends on the connection to the site.

2) Why is there a 39 second time gap between the first ECID on page 2 of the NIT report and Page 3 of the NIT Report and why is there a 63 second gap for the second ECID? What were the times to execute during their testing?

Unable to answer this

3) Does the Team know the NIT report is being used to support a Visit progression to the TB2 site? And that the Visit progression is "enter site, click on first url, then click on second url." If this was true, wouldn't the NIT Report referer for ECID #1 be the sites index page and the girls.html page for ECID #2?

4) Therefore, Why are the request_uri and the referer the same for each ECID?

I think those are from the logs of the site, not the NIT. NIT just sends back the session id.

Doesn't that indicate independent reloads of each page?

5) Could the reloads have occurred in hidden iframes and the user of the browser never even saw the two pages?

Lots of things could have occurred, but we would doubt it was a hidden iFrame. .

Servers don't save logs of the content of the files they send, only the files that are requested so it would be hard to determine. If we know the pages he purportedly visited we could inspect the source on the web servers and look for anything out of the ordinary.

6) How could gallery.swf fill out the blank fields on Page 3? Specifically, Updated TBB (Tor Browser Bundle)?

I think these were in the apache logs, not the gallery.swf.

We are not sure what he is asking. Since we don't know which version of TBB he used, or anything about the client, we can say that it necessarily came from him, only that the flash app is able of producing output as the FBI reported. If we had an unencrypted view of his system would could tell more about this.