With respect to the computer code identified on page 3 of the document attached to my September 4, 2014, e-mail, the code therein consists of "example programming code" for the flash application, as my e-mail indicated. The compiled code for the NIT resides on the (b) (7)(E) and TB2 computer servers. Forensic images of those servers have been made available, and remain available, for inspection, review and analysis by a forensic expert of your choosing. If your expert would like to examine an image of those computer servers, let us know, and we will facilitate it.

(b) (7)(E)

With respect to your further questions about other technical matters:

(b) (7)(E)

I do not understand what you mean by "Adobe Flash version on Mac OS to Author the SWF files used to connect to a socket server outside TOR." Each defendant in this case may have been running a different version of Adobe Flash. That information would be available via an examination of an individual defendant's computer. We have made and will continue to make available for examination digital evidence seized from your clients' homes.

I am also not clear about your requests regarding the socket server and the web server. Again, the computer servers running (b) (7)(E) and TB2, which contain the compiled NIT code, remain available for your expert's inspection and review.

Thank you,

-Keith

From: JGross [mailto:(b) (6), (b) (7)(C)@tgplaw.com]
Sent: Wednesday, October 8, 2014 5:37 PM
To: Becker, Keith; (b) (6), (b) (7)(C); Joseph Howard; (b) (6), (b) (7)(C)
Cc: Norris, Michael (USANE); Chang, Sarah
Subject: RE: NIT information - cases 13-cr-106, 107 and 108

Keith,

I am preparing a motion under *Daubert* to challenge the admissibility of the technology supporting the NIT and do not want to make unnecessary work for either of us. Here, I am talking about formal discovery requests.

I expect all defense counsel to join in the motion. Specifically, I've talked with Stuart Dornan and Jerry Hug and know they will join a challenge. Thus, please consider this email requesting discovery related to the NIT and informing you of certain preliminary matters for you to consider. I believe at least Mr. Hug will follow up with an email to you agreeing with some or all of the matters discussed and perhaps making additional discovery requests.

As I understand your September 4th email below, you are reporting information from FBI SA (b)(6), (b)(7)(C) per FBI. I make that point because if this email is not intended to be confrontational to you on foundational matters that more properly are directed to the FBI and SA (b)(6), (b)(7)(C) per FBI

First, I understand from your 9.04.14 email that the FBI used the computer code identified on page 3 of the document that you attached to the email. So we are clear, I've attached that same document to this email.

Second, it is my understanding that Adobe altered the security model within that version of Flash in approximately 2008 so the code you reference on page 3 would not have worked on the application in 2012. I make this point so you can correct the record, if necessary, or verify that the code on page 3 is indeed the correct code used by the NIT in 2012. If your email is in error, please provide us with correct code information. That is crucial information to the defense.

Third, in addition to the ActionScript code there are other matters that need to be disclosed in order for a thorough evaluation of the NIT used in Nebraska in November

2012.

Please provide or produce the following information:

- PHP code;
- HTML code;
- Javascript code (Browser Scripting Language);
- ActionScript code (Flash Scripting Language);
- Adobe Flash version on Mac OS to Author the SWF files used to connect to a socket server outside TOR;
- A socket server written in Java, Perl, C++ or other programming language;
- The web server(s) (IIS and or Apache) running on Windows or Linux or Unix.

Keith, please provide me with a reply as reasonably soon as possible. I would like to have a motion filed before October 31. If we have disagreement on production then perhaps a conference with the Court would make sense. Ultimately, it may make sense to have a Rule 17.1 conference to discuss the timing of the hearing and here again we'd probably be looking at an omnibus hearing due to the common issues of fact and law. I would expect the *Daubert* hearing to involve complex facts presented by various expert witnesses and a deliberative period by the court that needs to be considered with respect to trial settings depending upon Judge Bataillon's ruling on the suppression motions.

Reply or call me with questions.
jfg

Joseph F. Gross, Jr.
Timmermier, Gross and Prentiss
8712 West Dodge Road
Suite 401
Omaha, NE 68114
(b) (6), (b) (7)(C)

From: Becker, Keith [mailto (b) (6), (b) (7)(C)
Sent: Thursday, September 04, 2014 3:01 PM
To: (b) (6), (b) (7)(C) ; Joseph Howard; (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) ; JGross; (b) (6), (b) (7)(C)
Cc: Norris, Michael (USANE); Chang, Sarah
Subject: NIT information - cases 13-cr-106, 107 and 108

Counsel:

Some of you have asked about further information pertaining to the NIT. The following information comes from FBI Special Agent (b)(6), (b)(7)(C) per FBI:

We originally found the NIT code on the website decloak.net. That website is no longer available but is viewable via the "Waybackmachine" on archive.org. It is also currently viewable at core.metasploit.com. Technique number five (Flash plugin) is the one in question. A link to a sample of the Flash application code can be found at the bottom of the websites previously referenced.

The technique utilized a Flash application that, when downloaded by a user and activated by their browser, made a direct TCP connection to a server that we controlled. Depending on the operating system and version of the user's browser, the connection would bypass the browser's configured proxy server and reveal the user's true IP address. In addition, the NIT also sent the user's operating system name and architecture type.

For ease of reference, I have attached to this e-mail a printout from an Internet archive, dated August 16, 2012, depicting the web pages from decloak.net referenced by SA (b)(6), (b)(7)(C) (the page at core.metasploit.com is no longer available) as well as the example programming code for the flash application itself.

From: Becker, Keith [mailto (b) (6), (b) (7)(C)
Sent: Thursday, December 04, 2014 11:00 AM
To: JGross
Subject: RE: Can I call you tomorrow?

Joe: Here's a quick cite for you from a District Court in the 8th on the thumbnail issue, which specifically distinguishes thumbs.db images from the Stulock line of temporary internet files cases.

United States v. Luken, 515 F.Supp.2d 1020 (D.S.D. 2007), aff'd, 560 F.3d 741 (8th Cir. 2009). Files found in thumbnails database were acceptable to show that defendant purposely saved or downloaded child pornography images onto computer's hard drives and viewed the images in a thumbnail view in order to establish knowing possession of child pornography.

-----Original Message-----
From: JGross [mailto (b) (6), (b) (7)(C) @tgplaw.com]
Sent: Thursday, December 4, 2014 12:04 AM
To: Becker, Keith
Subject: Can I call you tomorrow?

Keith
Can you let me know if you have 10 or 15 minutes to talk tomorrow?
I need to run a few thoughts past you before I talk with Cottom and it relates to thumbnails and how those files were created and stored on his hard drives.
Dan Meinke and I spent quite a long time discussing this and it's important to me that I understand this from the perspective of the government's case in chief before I talk with Cotttom.
Basically I found numerous child porn images in the thumbnail format located in the thumbnailcache.
So one question is whether there is any case law that would distinguish a thumbnail from any other CP. Put differently, can the government prosecute a CP case based on thumbnails? Another question relates to how those files are created. I understand these files are created after a user downloads or deletes a file. So, in that way, it's not like a temporary Internet file raising the possibility of an innocent download under the Stulock line of case law. Further it seems to me that because Cottom's hard drives are encrypted it is entirely possible that the "original" image was downloaded and stored encrypted as evidenced by the thumbnails.
Thanks.
jfg
Joseph F Gross Jr
669 North 57 Street
Omaha, Nebraska 68132
(b) (6), (b) (7)(C)